Global Journal of Politics and Law Research

Vol.9, No.5, pp.32-57, 2021

ISSN: ISSN 2053-6321(Print),

ISSN: ISSN 2053-6593(Online)

CRIMINAL PROTECTION OF THE PERSONAL ELECTRONIC DATA PRIVACY

Mamdouh Hasan Mani' Al-Adwan
Associate Professor of Criminal Law
International University for Islamic Sciences
Faculty of Sharia and Law
Amman/ Jordan

ABSTRACT: *The right to privacy is one of the most important rights associated with the legal personality, and the protection, processing, maintaining and non-disclosure of personal data and information to others is one of the most important and greatest forms of privacy or the sanctity of private life. Maintaining human secrets is the essence and basis of guaranteeing freedom of privacy against violating others, and here the role of the legal rules that govern and regulate issues of this protection appears through the legislations that they enact to ensure that they are not infringed or disclosed, and by establishing the deterrent punishment against the perpetrators of these acts.As a result of relying on modern technology in various aspects of contemporary life and the increasing in the amount of data possessed by the state and private institutions, this matter leads the legislator to carefully consider how the data that contains information about individuals is collected and saved and the possibility of violating their privacy that may result through misuse it. Therefore, the urgent need has arisen to criminalize the illegal collecting of personal data, disclosure it, or unlawful transfer it.*

KEYWORDS: personal data, privacy, disclosure, criminalization, punishment.

INTRODUCTION

The emerging, renewable and developed technology raises problems day after day that need non-traditional legal solutions. Digital life results many problems related to legal existence in this virtual life.On the other hand, we find that the information trade has become one of the most important sources of wealth in the digital life, and among the aspects of it is the trade related to personal data because it is can be used politically, militarily and security.Therefore, the protection and regulation of using personal data is closely related to the protection of the constitutional right to privacy, therefore the legislations regulating the use of personal data are complementary to the Constitution.

The protection of privacy at the international level is attributed to the efforts of international and regional organizations, which had a significant impact on the drafting the legal system for personal data privacy. European law ranked first in this regard through the European Union's

General Data Protection Regulation, which represents a model law for many national legislations within and outside the European Union.

The protection of personal data is one of the most important elements of confidence-building in the digital space, and the safe use of information and communication technologies. The legal aspects of the privacy invasion represent through the illegal use of personal data in crimes and illegal acts committed by individuals or government agencies, including: Eavesdropping, extortion and hacking of information systems, access to professional and commercial secrets, in addition to the illegal monitoring of the movement of people and funds by government agencies, and drafting information files without a legal reason.The source of the danger in the invasion personal data is due to the nature of technology, on the other hand, the absence of appropriate legislative and regulatory frameworks, and the inadequacy of traditional protection models.

The concept of personal data protection

Understanding the concepts mentioned in the Personal Data Protection Law, clarifying them and exploring them are necessary in this context, before going into dealing with the provisions of this law. As the ambiguity of some concepts leads to wrongly understanding and dealing with them, which greatly impacts on the goals and effects that the legislator desires to occur through the provisions of the law.

We would like to mentioned out that the study will be limited to investigate some essential concepts of protecting personal data (personal data, processing personal data) as follows:

First: The concept of personal data,

Second: The concept of personal data protection and identifying its parties

II. A. The concept of personal data

In order to obtain a clear and accurate definition of the concept of personal data, it is necessary to differentiate between personal data covered by legal protection and other data not covered by this protection. Not only that, but non-personal data must also be identified in order to differentiate it from the aforementioned data.

There is no doubt that national laws will facilitate the work of those in charge of collecting and processing personal data when they provide a specific definition of personal data[1].

[1] Stephen Allison, The Concept of Personal Data under the Data Protection Regime, Edinburgh Student Law Review, Volume 1, Issue 1, 2009, p. 2.

In this regard, it should be noting the multiplicity of types of personal data, as they are not limited and differ according to how they are viewed; some of which are personal data subject to law enforcement, and some are non-personal data are outside the scope of this protection.

Accordingly, we deal with the definition of personal data, then we deal with non-personal data that is excluded from the scope of legal protection, and finally we refer to non-personal data, which is of course excluded from the scope of legal data protection, and we allocate for each point a separate paragraph.

II. A. 1. Defining personal data

It means any data related to an identified normal person or who can be identified, directly or indirectly, by linking it with any other data[2].

It is also: "Any data related to an identified normal person, or who can be identified directly or indirectly by linking this data to any other data, such as name, voice, picture, identification number, or identifier via the Internet, or any data that identifies psychological, health, economic, cultural or social identity".

Article 4 of European Regulation (GDPR) defines "Personal data" as: it means any information related to identified normal person or identifiable person (The data subject); as the normal person is a person who can be directly or indirectly identified, in particular with reference to a determinant of identity, (an identifier), like name, social insurance number (identification number), web site or web ID data (IP or email address), or one or more of the body, psychological, genetic, mental, economic, cultural or social details of this normal person.

Some jurists criticized the definition of personal data and considered it too broad[3] noting that the analyzing big data would make the distinction between data that would make a person identifiable and those that make the person undefinable is worthless[4].

The French legislator also defines personal data in Article Two of the Information and Freedom Act (amended) as: "Any information related to a natural person whose identity is identified or who can be identified directly or indirectly is considered one of the personal data, whether his identity is determined by referring to his personal number or by referring to any personal detail related to him". According to the aforementioned definition, any information related to a normal

[2] Article 1 of Egyptian Law No. 175 of 2018 regarding combating information technology crimes, published in the Official Gazette - Issue 32 bis (c) in August 2018.
[3]Nadezhda Purtova (2018), The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology, 10:1, 40-81, DOI: 10.1080/17579961.2018.1452176, p. 3.
[4] O Tene and J Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, (2013) 11 Northwestern Journal of Technology and Intellectual Property 258, pp. 19-20.

person who can be identified is considered as a personal data that is subject to legal protection, as long as this normal person is identified, or it is possible to determine his identity in any direct or indirect way.

This indicates that data definition is considered as criteria by which it can be determined whether a certain piece of data is considered as a personal data or not, which will determine whether it will be subject to legal protection for personal data or not.

It should be noted that the legal protection of personal data is limited only to the personal data of normal persons, and therefore the data of the legal person is excluded from the scope of legal protection[5].

II. A. 2 Defining non-personal data

It can be benefited from reversing of the definition of personal data according to the law to define non-personal data as data by which it is not possible to directly or indirectly determine the identity of a natural person, or in other words that is not significant in determining, identifying and distinguishing the person from others.

Then, "non-personal data" means data that cannot reveal the person's real identity, including, for example, information about the gender, the type of browser he uses, or the type of car he prefers.

Naturally, the legal person's data is considered non-personal data. For example, the Egyptian legislator provided a definition of government data, which is non-personal data, in the Anti-Information Technology Crimes Law No. 175 of 2018, as he defines it: "Data related to the state or one of its authorities, its agencies or units, public bodies, independent bodies and regulatory agencies, and other public legal persons and the like, available on the information network or on any information system or on a computer or what like them".[6]

Hence, non-personal data is out the protection provided by the law, but this does not mean at all that there is no protection provided by modern legislation regarding processing operations, as this data is not left - as some might imagine - without legal frameworks that protect it, as there are many of them - Like government data - protected under various legislation.

[5] Dr. SamehAbd Al-Wahid Al-Tohamy, Controls of Personal Data Processing, "A Comparative Study of French Law and Kuwaiti Law", Journal of the Kuwaiti International Law College, Third Year, Ninth Issue, March 2015 AD, pp. 401-402.
[6] Article 1 of Law No. 175 of 2018 promulgating the Law on Combating Information Technology Crimes, Official Gazette, No. (32) bis (c), August 14, 2018.

II. B. 1 Defining sensitive personal data

According to Article 1 of the Egyptian law, sensitive personal data means "data that disclose psychological, mental, physical, genetic health, biometric data, financial data, religious beliefs, political opinions, or the security situation. In all cases, children's data is considered sensitive personal data".

There is an observation on the legislator's behavior in that he described some data as sensitive, and then changed the dealing with it, in terms of collection and processing, including physical or genetic data, and the latter considered by the European regulations within the categories of personal data, without differentiating between normal or sensitive data.

In this regard, the legislator considered all data related to children to be sensitive data, and it is a general term that naturally relates to any data of the child, even if it is considered as personal data (normal and non-sensitive), such as the name, the surname, the voice, and any other data that identifies him.

While we find that the European regulation does not contain a definition of the name of sensitive data, but rather definitions of some data in particular (Article 4, Clause: 11-13), besides the definition of personal data, it mentioned a definition for both genetic data, biometric data and health related data.

Hence, we note that the European regulation provided a special definition to clarify some data. (Article 4, Clause 14) of the regulation defines "biometric data" as meaning personal data resulting from a specific technical processing related to the physical, physiological or behavioral characteristics of a natural person, which allows or confirms the uniqueness of this natural person, such as face prints.

It also defined "Data Concerning Health" (Article 4, Clause 15) to mean "personal data related to the physical or mental health of a normal person, including providing health care services, which reveal information about his health status".

The Regulation also defines "Genetic Data" (Article 4, Clause 13), that "means personal data related to the inherited or acquired genetic characteristics of a normal person that provide unique information about the physiology or health of that normal person that particularly results from analyzing a biological sample from him".

We find that the European legislator, although it defined some data, did not class it under the name of sensitive data, and in this regard, the regulations stated that determining the sensitivity of data is a matter that is decided by the national legislation of each country of the union.

While the European legislator mentioned definitions of some data that the Egyptian legislator described as being sensitive without defining it, we find that both legislators did not define "financial data", and it might have been better to define these data in order not to be under the interpretation of the people subject to the law.

However, the Egyptian legislator's neglect of the defining the financial data leaving open the questions, as it may be understood that he intentionally overlooked them when he excluded the Central Bank and banks data (which focus on financial data) from the scope of its applying.However, this assumption may be an exaggeration because the term of financial data is too wide to be limited to banks financial data, and therefore even if this is the reason for neglecting the definition of this term by the Egyptian legislator, this is a failure that requires amendment or a definition to be attached to the executive regulations expected to be issued.Likewise, neglecting the defining of health-related data (whether physical, psychological or mental), genetic data, and biometric data may lead to difficulties in understanding and interpreting the text - narrowing or expanding - in the case of practical application in a way that does not fulfill its intended purpose.Also, even with definitions, there is still plenty of room for interpretations of law and jurisprudence.

II. B. 2. The concept of personal data processing and determining its parties

In this regard, we deal with the definition of processing and the terms associated with it, then we refer to the definition of the controller, the processor, and the holder of the data (as they are handling processing).

II. B. 2. 1. Defining the processing and terms associated with it

- Defining the processing

The Egyptian legislature defined processing as: "any electronic or technical process of writing, collecting, recording, saving, storing, merging, displaying, sending, receiving, circulating, publishing, erasing, changing, modifying, retrieving or analyzing personal data using any tool, electronic devices or technology, whether this is partially or totally".

Regarding this definition, it would have been better if the Egyptian legislator had get away from using the term "electronic" and he refer to processing as "technical" processes[7] in order to control the accuracy of the formulation[8].

[7] The report of the Legislation Department of the State Council in this regard indicates that the term "technology" linguistically means: "any technical process based on dealing with electronic computers and computer software to transfer, store, protect and process data and information" while the word "electronic" refers to all electronic media and devices that these technical processes and procedures can be took place. Refer to the book of the Chancellor /

On the other hand, Article 4 of the European Data Protection Regulation defines "processing" as: "Any process or set of operations performed on personal data or on sets of personal data, whether by automated means or not, such as collecting, recording, organizing, structuring, storing, adapting, changing, retrieving, consulting, using or disclosing by transmission, publication, availability, alignment, merging, restriction, erasure or damaging".

Therefore, the processing of personal data includes any actions related to the data regardless of the method used in this procedure, any action taken in relation to personal data is considered processing of this data[9].

- Other terms related to processing concept

Both the term profiling and coding are acts that can be mixed with or related to the concept of data processing and defined by the legislation regulating the protection of personal data.

On the one hand, the European legislator has given a special definition of what is called "profiling", which means, as stated in Article 4 Clause 4 of the Regulation, that: "Any form of automated processing of personal data consisting of using personal data to assess certain personal aspects related to of a normal person, and in particular to analyze or forecast aspects of that natural person's performance in business, economic condition, health, character, preferences, interests, reliability, behavior, location, or movements."

The regulation also specified a definition of what might be called the "filing system". According to Article 4 of the Regulations, the filing system means: "any organized set of personal data that can be accessed according to specific criteria, whether it is centralized or decentralized or on a functional or geographical basis".

Vice President of the State Council and Head of the Legislation Department No. (24) dated January 16, 2020 attached to the report of the joint committee regarding "a draft law issuing a law on the protection of personal data", amending the definition of processing, pp. 109 and p. 125

[8] The Legislation Department of the State Council had proposed this when the draft law was presented to it. However, the legislation sector at the Ministry of Justice rejected this proposal, reasoning that the definition of processing by including an electronic term is an identical definition with the definition of electronic processing contained in Law No. 175 of 2018 regarding combating the information technical crimes, which defined it as: "Any electronic or technical process that takes place in whole or in part to write, collect, record, save, store, merge, display, send, receive, circulate, publish, delete, change, modify, retrieve, or derive electronic data and information, using any tool, computers, or other electronic, magnetic or optical devices, or what is developed from other technologies or media". The sector also added in its response that the standardization of technical definitions It is the basis for drafting legislation. Refer to: the book of the Chancellor / Vice President of the State Council and Head of the Legislation Department No. (24) dated January 16, 2020 referred to, pp. 109 and p. 125.

[9]Sophie Pena Porta, Les Donnéespersonnelles et leurtraitement, Art disponible sur www.pedagogie.ac-aix-marsille.fr, la date de miseenligneest: 2 mars 2005.

Processing operations that are considered as profiling or filing, although they are not criminalized in themselves, must follow the controls established by the legislation regarding data processing.

In evidence of the importance of these terms, we find that the failure of Hennes&Mauritz (H&M) to follow the necessary legal procedures when conducting processing operations, specifically profiling and filing, cost it huge sums recently in October (2020), when the Hamburg Commissioner for Personal Data Protection and Freedom of Information imposed a fine of 35.3 million euros to the company for violations of its employees' personal data, as the company collected and kept records of its employees containing data with a high level of privacy and for long periods of time.This data was also used in evaluating the performance of employees and creating detailed profiles for them to be used and depended on in taking decisions towards them. It is worth noting that the employees had no idea about this until a technical error occurred in the company's computer systems, which made this data available for several hours in October of last year[10].

On the other hand, the European Regulation provided a specific definition of Pseudonymisation, not for subject it to legal protection, but to take it out of the scope of personal data, and defined it as: “Processing personal data in such a way that it can no longer be linked to a specific person who is the subject of those data without using additional information, provided that such additional information is kept separately and that such additional data is subject to technical and organizational measures to ensure that it is not affiliated with an identified or identifiable normal person”.

In contrast to profiling and filing, which are like processing personal data covered by the protection regulation, we find that the pseudonymization of data is outside the scope of protection of the Data Protection Regulation (GDPR) because it does not lead to the identify the data subject[11].

It is worth noting that although there are some differences between the definitions of processing that we have mentioned, all of these definitions still need for more clarification and interpretation, and therefore we address some interpretations of the European Court of what is

[10]Hamburg Commissioner Fines H&M 35.3 Million Euro for Data Protection Violations in Service Centre; https://edpb.europa.eu/news/national-news/2020/hamburg-commissioner-fines-hm-353-million-euro-data-protection-violations_en Last Visited on the 19th of October 2020.

[11]GDPR, Recital (26): "The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person".

meant by processing, in an attempt to find out the meaning of that term and thus, determine the scope of protection of those personal data legislations.

- Applications of processing definition in European Court judiciary

The European Court of Justice, in many of its rulings, has dealt with the interpretation of the term processing and mentioned some acts that constitute processing of personal data. It first addressed the interpretation of the processing definition in 2003 in the Lindqvist case[12] when it stated that publishing personal data on a web page constitutes processing that makes it in this case is included under the protection of European Directive 46/(95)[13].

The court also indicated in a subsequent ruling that collecting, publication and transmission of personal data on CD-ROM or by text messages are all forms of processing personal data regardless of whether the published data has been modified or not[14].

It is worth noting in this regard that the European Court, in a recent judgment issued in 2014, refused to consider the legal analysis carried out by a party to respond to a request submitted by the data subject as personal data[15], but nevertheless decided that this does not conflict with the fact that the delivering of personal data was made in response to a request to obtain such data, which is considered as processing[16].

The court also stated in a well-known ruling that alteration or modification of personal data is in itself an act of processing, however that other data processing operations may arise without being modified.

The court also indicated that the ability of the search engine to "make available" data about the history and details of the search that a person may perform, is a form of processing, as is the case

[12]ECJ, Case C-101/01, 6th November 2003; [2003] ECR 1-12971), Found at: http://curia.europa.eu/juris/liste.jsf?num=C-101/01.

[13]The term personal data used in Article 3(1) of Directive 95/46 covers, according to the definition in Article 2(a) thereof, any information relating to an identified or identifiable natural person. The term undoubtedly covers the name of a person in conjunction with his telephone coordinates or information about his working conditions or hobbies. Paragraph (24), (ECJ, Case C-101/01, 6th November 2003; [2003] ECR 1-12971).

[14]ECJ, Case C-73/07, 16th of December 2008, Tietosuojavaltuutettu [Finnish data protection ombudsman] v. SatakunnanMarkkinaporssi Oy and Satamedia Oy, 16.12.2008 ("Tietosuojavaltuutettu").

[15]Joined Cases C-141/12 AND c372/12 YS v. Minister VoorImmigratieIntegratieenAsiel and Minister VoorImmigratie, Integrate enAsiel V. M, S (2014).

[16]C-28/08, Commission V. Bavarian Lager CO., 29.6.2010 ("BAVARIAN LAGER").

with all operations prior to availability, such as the collecting, recording, organizing and storing such data by a search engine automatically, continuously and systematically[17].

The court did not neglect the processes related to the latest technological developments and dealt with the interpretation of the term processing, as it touched on the process of collecting and storing fingerprints and classified them as falling within the framework of processing[18].

II. B. 3. Definition of the controller, the processor and the holder of the data (the ones in charge of the processing operations)

The Personal Data Protection Act includes definitions of the processor, controller and holder, and in this way they are in line with the definitions contained in the European Data Protection Regulation (GDPR).

In the following, we will discuss the definition of both the controller and the processor, in addition to the specificity of the concept of the holder in, as follows:

- Controller definition:

The Egyptian legislator defined the "data controller" in Article 1 of the law as "any normal or legal person who, by the virtue or the nature of his work, has the right to obtain personal data and to determine the way, method and criteria for keeping it, or to process and control it according to the specific purpose or activity".

The European Regulation defines "controller" as: "a normal or legal person, public authority, agency or any other body that determines, alone or jointly with others, the purposes and means of processing personal data; Where the purposes and means of such processing are established by Union or Member State law, the controller or the criteria for determining it may be determined by Union or Member State law" (Article 4 Clause 7).

The European Regulation referred in Article 26 to the issue of "Joint Controllers" by: "1- When two or more controllers jointly specify the purposes and means of processing, they shall be joint controllers, and their responsibilities for compliance of the obligations under this regulation shall be determined in a transparent manner, in particular for the exercise of the data subject rights and their respective duties to provide the information referred to in Articles 13 and 14, by means and in arrangement between them unless the responsibilities of each controller are specified under

[17]C-131/12, GOOGLE SPAIN SL V. AEPD (THE DPA) & MARIO COSTEJA GONZALEZ, 13.5.2014 ("GOOGLE"), Paragrapghs 26-31"

[18]C-291/12, Schwarz v. Bochum, 17.10.2014 ("Schwarz"), Para 28-29.

Union law or the law of the Member States to which the controllers are subject, and the arrangement may allocates a point of contact for data subjects.

The criterion for the existence of joint control in the participation of two or more entities in determining the purposes and means of the processing process, and joint control can be embodied in the form of a joint decision taken by two or more entities or resulting from close decisions by two or more entities, where the decisions are complementary each other and are necessary for processing , so that it is carried out in a way that has a significant impact on determining purposes and means of processing.In addition to the necessity of participating both parties in the processing, and that the joint control process includes defining the purposes on the one hand and defining the means on the other hand[19].

In contrast to the European Regulation, which briefly addressed the necessity of determining liability between joint controllers, the Egyptian legislator did not refer to any conditions for joint control and did not provide for the possibility of designating a focal point to facilitate access to the controller rather than placing this burden on the person concerned with the data.

This difference between the legislation can be explained by the fact that the Egyptian legislator has included in the data protection law what he considers the minimum required protection, and accordingly the parties are not allowed to agree on dividing these obligations or transfer some of them to another person, rather each controller must obligate to them in order to provide a greater degree of protection for the data subject who can refer to any of them to arrange responsibility.However, there are still practical considerations that may raise problems under the absence of regulation and criteria for joint control. For example, to determine the extent to which one of the data controllers may decide to reuse the data for a new purpose, and is there a need to obtain the approval of the other controller?

- Definition of processor

Egyptian law (Article 1) defines a “data processor” as “any normal or legal person competent in the nature of his work, to process personal data for his benefit or for the benefit of the controller in agreement with him and according to his instructions”.

It is noted that the report of the joint commission had amended this definition in the bill submitted by the government by deleting the part that makes the person processing the data in his favor a processor. The text proposed by the committee was as follows: “Any normal or legal

[19]Guidelines 07/2020 on the concepts of controller and processor in the GDPRErpoian Data Protection Board Report. 2020.

person concerned with the nature of his work in the processing of personal data, for the benefit of the controller and in agreement with him and according to his instructions"[20].

The workshop considers that it would have been better if the final text of the article was similar to the text proposed by the joint committee, because there is no need to mention the ability of a person to process data for himself, because that makes him controller.

Whereas a Processor is defined by European Regulations (Article 4 Clause 8) as "means a normal or legal person, public authority, agency or other body that processes personal data on behalf of the controller".

It appears from this that there is a partial difference in the definition of Egyptian law and the definition of the European regulation forthe processor, where the Egyptian law allows the processor to perform the "processing process" for its benefit and not for the benefit of the controller, while the definition of the European regulation limits it to performing the processing on behalf of the controller.The question arises here about the responsibility of the processor in the event that he performs the treatment process for his benefit, not based on the instructions of the controller, and about the aim of the Egyptian legislator from adding the possibility of processing in favor of the processor.

In general, both Egyptian law and European regulation agree to define the controller-processor relationship by defining who has the decision-making authority regarding processing of personal data, i.e. who has the authority to determine the purpose and the method of processing[21].

Based on the above, the processor must not process the data contrary to the instructions of the controller, and the controller has the absolute authority to set the frameworks and purposes of the processing, allowing the processor to choose the most appropriate technical and organizational means to serve the primary purpose for which the data is collected. However, the processor is not allowed to violate the instructions of the controller[22].

Here are some examples that illustrate the work scope of each one, to illustrate the difference between what is meant by a processor and what is meant by a controller:

[20] Report of the joint committee of the Communications and Information Technology Committee and the offices of the constitutional and legislative affairs committees, previous reference, pp. 14 and 32.

[21]Rowenna Fielding, 'The Concept of Controller and Processor Data Entities' (2018).

[22]The concept of "controller" under the Personal Data Protection Act and the GDPR is similar to the concept of "company" or "commercial organization" in the California Consumer Privacy Act, as both have decision-making power regarding the processing of personal data. Also the concept of "Processor" in the Personal Data Protection Act and the GDPR has similarities with the term "Service Provider" under the California Consumer Privacy Act.

In the case of dealing with customer data within the framework of providing electricity services, we find that the service provider under a contract with the person concerned with the data is the Electricity Company, which in this case is considered to be the data controller, while we find that the data processing for extracting the bills is not carried out by the same company in Egypt, but rather by another company, in which case the latter is a data processor only without being in control of it.

The workshop also referred to the case of processing personal data within the framework of providing air transport services. In this regard, the air transport service is provided by EgyptAir, which obtains the personal data necessary to provide the service and deals with it as a controller, while we find that the process of processing that data to extract tickets for flight travels is carried out by another company (Amido), which in this case is considered as a data processor.

III Rights of the person who is data subject and terms of data processing

The normal person whose personal data is collected and processed, or what is known as the data owner or "data subject", is one of the primary parties in the data processing process.

III. A. Defining the person who is data subject

The main trigger point in clarifying the rights and obligations of this person lies in defining him in a manner that defines his identity. For this reason, the Egyptian law defines him in Article 1 of it as: “Any normal person to whom electronically processed personal data is attributed, that indicates to him legally or practically, and which enables distinguishing him from others”.

Article 4 of the European Regulation defines a “Data subject” as “a normal person who can be defined or can be identified directly or indirectly, in particular by referring to the identification number or to one or more factors determining his physical, physiological, mental, economic or social identity[23].

It appears from these definitions that the person concerned with the data is every normal person whose personal data is the subject of collecting and processing based on sound consent, unblemished by any defects of will.

The investigate in this axis can be divided as the following:

1. Clarify the rights of the data subject
2. Procedural aspects of exercising the rights of the data subject.
3. Terms of legality of collecting and processing personal data.

[23]The French legislator defines him in the amended Law on Information and Freedoms as “every normal person whose personal data is the object of processing (Article 2).

III. A. 2. The rights of data subject

The rights of the data subject are listed in the European GDPR Regulation in its third chapter (Articles 12-23).

In fact, it must be recognized that acknowledging for the data subject with some rights over his data is a basic goal pursued by the law, in order to provide him with effective legal protection as he is the main purpose of this protection.

The most important rights that the normal person who is data subject can be provided with over his personal data, we list them as follows:

- The right to know, view, access or obtain personal data

The data subject was giving the rights to know, access or obtain his data with any "holder, controller or processor", and the European regulation called it the Right of access to data, where it stipulates in Article 15 that the data subject has the right to obtain confirmation from the controller whether the personal data relating to him is being processed or not,If this occurs, he shall have access to the personal data and the following information: Purposes of processing - Categories of personal data concerned - Beneficiaries or categories of recipients to whom personal data has been or will be disclosed, in particular beneficiaries in other countries or international organizations - The period during which personal data is stored or, if this is not possible, the criteria used to determine that period -The existence of a right for controller to request correction or erasure of personal data, or restricting the processing of personal data relating to the data subject, or objecting to such processing.

In fact, there is several types for the rights of data subject, which are:

- The person whose data has been collected and processed shall have the right to be aware of his data that is with any holder, controller or processor. It is recognized that knowledge, in language, is a source of the act of knowing, which is the realization of the thing as it is, that is, its definitive realization of what it is, it is also knowledge and certainty, which is the opposite of ignorance.

The personwho is data subject has the right to view and access his data: this right requires enabling this person, his heirs, or his legal representative to access all his data subject of processing, and this right may not be waived or limited except within the limits of the law.

The right to discover and access to the data is linked to the right to obtain it, as it is expressed in that text, and this means the right of the person to obtain a copy of his data in a clear language and in conformity with what is in the possession of the controller and others, upon his request, in accordance with the established procedures, and pay financial reimbursement for this the service.

- The right to withdraw consent to keep or process the data.

It is required that an explicit consent be issued by the data subject for the data collecting or processing operations, except in the cases authorized by law, and therefore it is understandably for the person to withdraw this consent, i.e. withdraw his consent at any time, as it relates to his rights that are closely related to his personality,as private matters may occur with person that require not keeping or processing the data.

The withdraw request is issued by the person himself or by any legal person (such as heirs or his representative) and is directed to the controller, processor or holder, and he must make decision about it, within a reasonable period, and this withdrawal results in the inadmissibility of the controller or processor saving or processing the data.

The European Regulation established the right to withdraw of consent in the third paragraph of Article 7 thereof, allowing the data subject to withdraw his consent at any time. However, the withdrawal of consent does not affect the legality of the processing carried out based on the consent prior of its withdrawal, provided that the data subject must be informed of this before the consent is given, and the withdrawal of consent must be facilitated.

- Right to correction, modification or erasure of personal data:

This right includes multiple images, including correction, modification, delete, addition or update of personal data.

It is worth noting that the phrased of these words involves unnecessary repetition, as correction, addition or updating are issues in themselves that fall under the description of the amendment, and there is an amendment by addition, deletion, correction or update.

- Right to rectification: The data subject, or any person with such capacity, shall have the right to request data rectificationif it contains errors during its collection and processing.

He may also amend this data, whether by adding or updating this data if it contains a deficiency or changing, and whenever it is inaccurate, incorrect, misleading or ambiguous.

Article 16 of the European Regulation provides for the right to rectification, indicating that the data subject has the right to obtain from the controller without undue delay the rectification of inaccurate personal data relating to him and, taking into account the purposes of the processing, he must have the right to complete the missing personal data, using means including by providing an additional statement.

- The right to erase (Right to be forgotten): The Internet, and its associated huge servers under the control of giant companies, is characterized by its voraciousness to collect and store

information, and its absolute memory in which what is stored in it cannot be easily erased by users, which makes natural forgetting is difficult to achieve at the present time, as it limits its users with their activities, whether in the form of comments, private news, photos or personal information, it also collects and records their data and information, and stores and retains it for an unlimited period, with the availability of this data and information from anywhere in the world and for everyone He wants and at the time he likes, knowing that this data and information may be outdated, erroneous or incorrect, yet it remains available to everyone and always indefinitely.

These risks can expose the data subjects to very serious harm and constitute a clear threat to their privacy, and their right to have their data erased with them online. This prompted legal thought to search for solutions to this problem to protect the privacy of people, and it found its value in the concept of "the right to be forgotten" in the digital environment, as one of the rights associated with the sanctity of human private life.

Therefore, the Egyptian legislator (Article 2 of the law) stipulates the right of the data subject to erase his personal data, and the right to erasure is called "the right to be forgotten" or the right to enter into oblivion, or the right to digital forgetting[24].

This right means that every person has the right to permanently delete the personal data saved by the processor, controller or holder upon canceling or leaving the service or application, and not to keep any copy of it for any reason, including removing links that lead to information about him on the Internet like (search engines, websites, social media sites...), it also means the obligation of those responsible for processing or saving personal data that they do not save such data for a period exceeding the purpose for which it was collected[25].

This right has received great attention in Europe, especially after the European Court of Justice Judgment No. C-131/12 of May 13, 2014 against the search engine "Google"[26], where it

[24]For more details on this right, see: d. Abdul-HadiFawzi Al-Awadi: The Right to Fall into Oblivion on the Internet, Dar Al-Nahda Al-Arabiya, first edition, 2014 and also:Maxime BESÈME:Le droit à l'oublinumériquedans le droit de l'Unioneuropénne, Consécrationprétorienne et legislative,Mémoire UCL) Universitécatholique de Louvain, (2015-2016.Disponiple sur Internet:https//:dial.uclouvain.be/memoire/ucl/en/object/thesis:7609/datastream/PDF_01/view.

[25]The National Informatics Committee in France defines the right to digital oblivion as the right to control in time over personal data, in order to obtain its deletion or erasure when so desires.

[26]European Court of Justice Judgment No. C-131/12 was issued on May 13, 2014, in a case known as the Mario Costega case against Google Spain and the main Google in the United States of America, in which the court ruled in favor of Internet users' right to require search engines like Google to remove search results for personal data, whenever the links in question are "inadequate, irrelevant, no longer relevant or exaggerated", even if the content is valid and legitimate as long as data subject wishes to forget them. The Court based its decision on the provisions contained in European Directive No. 95/46 on the protection of the processing and transfer of personal data, as

recommended the European legislator to provide guarantees to protect this right, and he responded for this demand, where he expressly recognized this right in Article 17 of the European Data Protection Regulation, where it indicates in the first paragraph that the data subject has the right to oblige the controller to delete personal data relating to him without undue delay, and the controller must delete the personal data without delay.

Accordingly, the European user was able to require Internet companies about his right to erase his personal data and respect his right to enter into digital oblivion[27].

- Reasons for applying the right to be forgotten:

The European legislator specified the cases in which the right to erasure applies, or what is called the right to be forgotten, in the European regulation, where Article 17 of it included clear provisions regulating this right,it requires one of the following reason in order to apply the right to be forgotten:

- Personal data is no longer necessary in connection with the purposes for which it was collected or processed;
- The data subject's withdrawal of consent on which the processing is based in accordance with the first paragraph of Article 6, or the first paragraph of Article 9, and where there is no other legal basis for the processing;
- The data subject objection to the processing in accordance with Article 21/1 and there are no legitimate grounds justifying the processing, or his objection to the processing in accordance with Article 21/2;
- if the personal data is illegally processed;
- Personal data must be erased to fulfill a legal obligation in the law of European Union or Member State law to which the controller is subject;
- Personal data was collected in relating the provision of information society services referred to in Article 8/1.

well as the European Convention on Human Rights of 1950.For more details see: Al-Salihin Muhammad Al-Aish, Commentary on the ruling of the European Court of Justice of May 13, 2014 regarding the right to consider some facts in limbo, research published in the Journal of the Dubai Judicial Institute, No. 5, February 3, 2015, pp. 169 et seq.; Dr.Moaz Suleiman Alma: The idea of the right to enter into digital limbo in modern electronic penal legislation; A comparative study between French penal legislation and Kuwaiti penal legislation, Journal of the Kuwait International Law College, Research of the Fifth International Annual Conference, May 9-10, 2018, Special Supplement, No. 3, Part One, May 2018, p. 117 and beyond.

[27]() In this regard, it is indicated that Google has included in its Transparency Reporting Policy that the users of its engine are advertised abot European Privacy Law impact on Google search results, "Requests to remove content under European Privacy Law", and requests to remove URLs from Google Search to preserve privacy, at its following site:https//:transparencyreport.google.com/eu-privacy/overview?hl=ar&hl=es

If the controller makes personal data available to the public and is obligated to erase the personal data, it shall, taking into account the available technology and the cost of implementation, take reasonable steps, including technical measures, to inform the controllers of personal data processing that the data subject has requested the erasure of any links they have or copies of this personal data (Article 17 paragraph 2. ER).

- The fields of applying the right to be forgotten

The field of applying the right to be forgotten is limited to the digital environment with regard to electronic traces or digital memories, which are all data and information related to a person and his activity of using an information activity or electronic means of any kind (social media - search engines - blogs - e-commerce sites ... and others) that would contribute to defining his digital identity, and the person's opinions and his contributions on the Internet of any kind are considered among the digital traces.

More recently, the European Court of Justice ruled, on September 24, 2019, that if Google is required to withdraw links at the request of a regulatory body or court in an EU country from all of its European websites, the online “right to be forgotten” stops there, and therefore it is not required to apply this right to its search engines outside Europe.

The court indicated that EU law does not require search engine operators such as Google to carry out such link's removal on all versions of its search engine.

But it concentrates that links removal from European sites should include measures that "seriously discourage" the European Internet user from being able to circumvent the "right to be forgotten" by accessing unfettered results via a search engine in a domain outside the European Union, and this requires imposing " Geo-blocking", which Google says that it implements it effectively in Europe.

The workshop recommends: to law edits the text regarding identify a certain period during which data must be editing or deleting as what some laws required[28].

The workshop recommends that: The executive regulation includes the conditions and controls for exercising these rights (the right to correct - the right to amend - the right to erase or “forget”), precisely.

- Right to allocate processing within a specified scope (treatment limitations):

[28] The Moroccan law has identified the period for normal persons’ protection toward processing personal type data, Article 1/8, is 10 days.

The European regulation includes this right in Article 18 of it, as this is taken into account by the European Regulation, and actually implemented by companies and entities subject to its scope of applying, where a person may request the limitation of processing his personal data according to the following conditions:

- If he objects, the accuracy of his personal information for a period of time enabling the responsible person to verify the accuracy of the personal information;
- If the processing is unlawful, and the data subject refuses to delete the personal data and instead he requests to limit of using the personal data;
- If the responsible person no longer needs personal data for processing purposes, but the data subject needs it to assert, establish or defend legal claims.
- If the person objects to the processing in accordance with Article 21 paragraph 1 of the European Regulation, and it has not yet been determined whether the legitimate reasons of the responsible person outweigh those of the data subject.

When the processing of personal data relating to the data subject is limited, such data may only be used with his approval (except for data storage) for the purpose of asserting or establishing legal case, defending them or protecting the rights of another normal or legal person or for reasons of significant public interest of the European Union or the State Member.

If processing is restricted in accordance with the above conditions, the person in charge will inform the data subject before lifting this restriction.

The workshop recommends: It is important that the Executive Regulations take into account the controls for exercising the right to restrict processing, similar to the European Regulation.

- Right to be informed of any breach or busting of personal data:

This right is considered axioms, as it is natural to oblige the controller or processor to notify the data subject of what may happen to this data, and the attacks that may occur to it, in any form or with any means.

The identification of data breach is useful for the data subject to manage his affairs and make a decision that is in his best interest, as he may withdraw his consent or request to amend or correct the data when any distortion occurs, or request to completely delete data.

- Right to object to the processing of personal data:

According to Article 21 of the European Data Protection Regulation, any person has the right at any time to object to the processing of his personal data right to object in accordance with the first paragraph of Article (6) clause (e) or (f) of the Regulation for reasons arising from his own

situation; This also applies to setting up profiles on the basis of these provisions.Hence, the responsible person may not then process the personal data related to the data subject unless he can prove compelling legitimate reasons for the processing that outweigh his interests, rights and freedoms, or that the processing aims to institute legal proceedings.

If the personal data relating to the data subject has been processed for direct marketing purposes, he has the right to object at any time to the processing of his personal data for the purposes of this advertisement; This also applies to setting up profiles as long as it is associated with this direct mail. If the data subject objects to the processing for direct marketing purposes, then his personal data may not be processed for these purposes (Article 21/2, 3 of the Regulations).

Regardless of Directive 2002/58/EC, the data subject has the option, in the field of using the information society services, to exercise his right of objection through automated procedures that use technical specifications (Article 5/21 of the Regulations).

When personal data is processed for research, historical or statistical purposes, in accordance with Article 89/1, the data subject has, for reasons related to his particular situation, the right to object to the processing of his personal data, unless the processing is necessary to perform a task being carried out for purposes of public interest (Article 6/21 of the regulation).

- Right to data portability:

The European legislator did not forget to stipulate this right to data portability in the European Regulation, as it was included in the Article 20 of it, which is that the data subject has the right to receive his personal data that he provided to the responsible person in a structured, known and machine-readable format.In addition, you have the right to portable this data to another person responsible for it without hindrance by the person responsible for providing the personal data, provided that:

- Processing is dependent on consent as indicated in Article 6 Paragraph 1 Clause (A) of the Regulations or Article 9 Paragraph 2 Clause (A) of the Regulations or on a contract in accordance with Article 6 Paragraph 1 Clause (B) of the Regulations.
- Processing is carried out by automated means.

By exercising this right, the data subject also has the right to verify that his personal data is being transmitted directly from one person to another, as long as this is technically feasible, and the freedoms and rights of other persons shall not be affected.

The right to data portability does not apply to the processing of personal data necessary to perform a task under public interest purposes or to exercise the official authority delegated to the responsible person.

III. A. 2. The penal framework for personal data protection

The penal legislature has tended to diversify its punitive tools to ensure itself flexibility in facing the various possibilities of personal data breaches[29].Therefore, the providing for penalties was according to two types of penalties for different crimes: financial penalties represented in fines of varying amounts, and freedom-depriving penalties and their form of imprisonment.

By extrapolating the texts of the data protection law, it appears that the legislator has taken financial penalties, specifically fines, as a primary tool to deal with threats to personal data. The punitive provisions, from Article (35) to Article (48) of the law, have made fines as a common factor among them, as fines were stipulated as a basic or only option in all articles.

The European Regulation (Article 83 Clause 4) has adopted a single division of fines. According to this division, the maximum fine is ten million euros or 2% of the entity's gross annual income in certain cases, and the fine in other cases is raised to 20 million euros or 4% of the total income as a maximum (Article 83, Clause 5).In this regard, we address the reflection of the distinction between ordinary and sensitive personal data on punitive treatment, the scope of fines and their effectiveness in general, and then we will address the phenomenon of duplication of criminalization texts.

- Distinguishing between normal and sensitive personal data in term of penal treatment:

We find that the penal legislation is extensively concerned with giving more protection to sensitive personal data, as it not only imposed more restrictions on processing operations that include sensitive personal data, but it also extended this protection to include more severe penalties for violations related to it.

Also, for normal personal data, the penal legislator has made a distinction between the case of illegal handling of ordinary personal data - mentioned previously - that is carried out for a purpose of a financial or moral return, or to expose the person to danger or harm, and the case of a dealing that takes place for other purposes.This distinction has a great importance, as it addresses one of the biggest threats facing personal data, which is data trafficking, and similarly it deals with the malicious purposes of personal data processing such as endangerment or harming.

[29]Hossam Muhammad Nabil Al-Shanraqi: Protection of Personal Data via the Internet: Challenges and Solutions, The Arab Journal of Management, Supplement, Issue Two, Volume 38, 2018, p.

Addressing that behavior is one of the goals for which the law was formulated in the first place; As when it aims to protect personal data in general, it wants to protect it from the challenges posed by technology in particular, which made the circulation and access to that data much easier, and thus the opportunities to benefit from and invest this data became greater than before, and it became a raw and attractive material for trading and dealing with it for different purposes.

Therefore, it was necessary for the legislator to have a firmer stance about the issue of the illegal processing of personal data carried out with the aim of obtaining a return, so that such data does not become a tradable commodity. The areas that may depend on personal data and therefore require dealing with this data are too diverse to be presented, but for example, personal data is a very valuable commodity in the field of commercial marketing that you may pay huge amounts for.The same applies to the use of data for political purposes and an attempt to understand and influence the political arena. An example of it is the famous Cambridge Analytica case, in which the personal data of Facebook application users was used to design the presidential election campaign of one of two candidates to suit the trends of the voter base[30].

This distinction in penalty based on the purpose of a data breach has not been applied to sensitive data. As the penalty, or more precisely the scope of the penalty, is the same regardless of whether that unlawful processing was done for a return or with the intent of endangering or harming a person. That is, any infringement of sensitive personal data is subject to a single penalty, whatever the intention of the dealer in that data.

This diversification of treatment between normal and sensitive personal data is therefore fit for purpose; There are two limits to the fine in normal data according to the purpose of the breach, which is commensurate with fact that it is the most widespread and most widely used and traded, and there is one limit for the fine for violating sensitive personal data to fully and more strictly protect it.

The scope of the fine is not the only punitive guarantee that the law attaches to sensitive personal data, but rather it broadens the objective scope of criminal acts that constitute a breach of sensitive personal data;As for normal personal data, “collecting, processing, disclosing, making available, and circulating” is criminalized in cases not authorized by law and without the consent of the data subject.As for sensitive personal data, other processes have been added to these actions, including “storage, transfer, and archiving.

[30]Final Order of the Federal Trade Commission of the United Stated of America in the matter of Cambridge Analytica, LLC, a corporation, docket no. 9383, issued at November 25, 2019; available at [https://www.ftc.gov/system/files/documents/cases/d09389_comm_final_orderpublic.pdf].

This raises the question; It is assumed within the scope of data protection that all types of personal data are protected against all operations that pose a threat to its security, and there is no difference in that based on the type of data whither it is normal or sensitive, as the difference is only in the guarantees of obtaining this data and the penalties for violating it, so that a higher level of guarantee is ensured to protect sensitive personal data, however threats should be addressed from the same perspective.

- The scope of fines and their effectiveness

By following the approach of the penal legislator when setting the minimum and maximum limits for each act, we can deduce the order of the legislator's priorities and the considerations that are most and least in need of protection in his view.The most serious violations are three: The first is violations that focus on sensitive data. The legislator also considered violating the provisions of licenses, permits and accreditation as among the violations that deserves the highest category of fines, whoever the violator is, which includes, by nature, the holder, the controller and the processor, as well as those who engaged in the activity of providing consultancy in the field of data protection. The third case involves violating the provisions of cross-border data movement.

On the other hand, the lowest category of fines is imposed on the holder, controller and processor who fail to obtain the consent of the data subject to carry out the processing, or if they do it without the legally authorized cases.

In general, it can be said that the legislator assigned the lowest level of the penalties for violations of the rights of the data subject. While in the middle are the penalties related to the obligations of the controller, the processor, the center's employees, the data protection official, and the violations related to the provisions of e-marketing.

This gradation of fines has been adopted by the GDPR. According to Article (83) of that regulation, fines are divided into only two categories: the first category, which imposes a fine which its highest value ranging from €10 million or 2% of the company's or organization's gross global income, while the second category with the higher value includes the fine between 20 million euros, or 4% of its turnover. These two categories do not have any minimum limits, which gives more flexibility to the authority concerned with imposing the penalty.

In general, the global approach to penalizing personal data breaches is based on a broad range of fines, specifically technology-related laws[31].The law also did not distinguish in punitive

[31]It is noted that the fines stipulated in the Personal Data Protection Law differ in their nature from those included in the European regulation, as the fine in Egypt is considered a criminal penalty while it is an administrative fine

treatment between large and small institutions, as it did not grant the latter any exemptions, reduced sentences, or lower fines. Accordingly, he has left the level of the punishment to the judge, and to what the executive regulations also include about it[32].

- The duplication of incriminating texts

By extrapolating the punitive texts in the data protection law, some confusion appears regarding some criminal acts. For example, the legislator considered the illegal act of "collecting" data carried out by controller with as criminal in two different places without apparent difference in the terms of applying with the difference in punishment.

The controller is obligated to obtain or receive personal data from the holder or controller or from the competent authorities to provide it to him, as the case may be, after the approval of the data subject or in the cases authorized by law. The obligation here also is included within the concept of data collection as well, so that there is unity in the subject and the person and a difference in the penalty, which represents a duplication in the texts of both criminalization and punishment.

CONCLUSION

Issuing legislation to protect personal data is a very important step to secure personal data, and an expression of the right of people to protect their personal data, and to criminalize illegally data collection or without the consent of the data subject.Therefore, it is necessary to develop mechanisms to address the risks arising from using personal data of people, and to combat the violation of their privacy within a legislative framework that copes with the increasing use of personal data.This is achieved by formulating obligations on the data controllers, and obligating the organizations, entities and individuals that control and process personal data to appoint an official of personal data protection to ensure the privacy of people.On the other hand, the legislative policy that is dealing with the infringement of personal data must be based on providing criminal protection through deterrent penalties, whether it is imprisonment or high fines and fair compensation to the right holder, because, as we mentioned, this constitutes a

according to the European Regulation, which results in the different jurisdiction to impose the fine in both systems. In Europe, data protection centers are specialized in estimating, impose and reduction the fine, while that jurisdiction is assigned to the court alone in Egypt. It also means that fines in Egypt as criminal fines are subject to all criminal penal rules; It is subject to the principle of legitimacy, and to the principle of the individual nature of the punishment, and it is multiplied by the multiplicity of the actors, which means the possibility of subjecting more than one controller or holder for a fine separately for the same act; Article (44), Egyptian Penal Code.

[32]https//:iapp.org/news/a/german-dpas-push-model-for-higher-gdpr-fines/111 – Paul Lambert, 'Data Protection, Data Loss and Penalties' (2012) 4 IBLQ 22, p 26;recital 13, GDPR.

blatant infringement of the right to privacy and affects it significantly in light of the broad spread of personal data that accompanied technical progress and the information revolution.

References

- Stephen Kai-yi WONG، Guobin ZHU Personal Data (Privacy) Law in Hong Kong A Practical Guide on Compliance, City University of HK Press,2021
- Christina Akrivopoulou & Athanasios Psygkas, Personal Data Privacy and Protection in a Surveillance Era: Technologies and Practices , IGI Global,2011
- Els de Busser, Data Protection in EU and US Criminal Cooperation,Makalu,2009
- Stephen Allison, The Concept of Personal Data under the Data Protection Regime, Edinburgh Student Law Review, Volume 1, Issue 1, 2009.
- NadezhdaPurtova (2018), The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology, 10:1, 40-81, DOI: 10.1080/17579961.2018.1452176.
- O Tene and J Polonetsky, Big Data for All: Privacy and User Control in the Age of Analytics, (2013) 11 Northwestern Journal of Technology and Intellectual Property 258, pp. 19-20.
- Dr. SamehAbd Al-Wahid Al-Tohamy, Controls of Personal Data Processing, "A Comparative Study of French Law and Kuwaiti Law", Journal of the Kuwaiti International Law College, Third Year, Ninth Issue, March 2015 AD, pp. 401-402.
- Sophie Pena Porta, Les Donnéespersonnelles et leurtraitement, Art disponible sur www.pedagogie.ac-aix-marsille.fr, la date de miseenligneest: 2 mars 2005.
- GDPR, Recital (26): "The principles of data protection should apply to any information concerning an identified or identifiable natural person. Personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be information on an identifiable natural person".
- C-131/12, GOOGLE SPAIN SL V. AEPD (THE DPA) & MARIO COSTEJA GONZALEZ, 13.5.2014 ("GOOGLE"), Paragrapghs 26-31"
- Guidelines 07/2020 on the concepts of controller and processor in the GDPRErpoian Data Protection Board Report. 2020.
- Rowenna Fielding, 'The Concept of Controller and Processor Data Entities' (2018).
- d. Abdul-HadiFawzi Al-Awadi: The Right to Fall into Oblivion on the Internet, Dar Al-Nahda Al-Arabiya, first edition, 2014 and also:Maxime BESÈME:Le droit à l'oublinumériquedans le droit de l'Unioneuropénne, Consécrationprétorienne et legislative,Mémoire UCL) Universitécatholique de Louvain, (2015-2016.Disponiple sur Internet:https//:dial.uclouvain.be/memoire/ucl/en/object/thesis:7609/datastream/PDF_01/view.

- Al-Salihin Muhammad Al-Aish, Commentary on the ruling of the European Court of Justice of May 13, 2014 regarding the right to consider some facts in limbo, research published in the Journal of the Dubai Judicial Institute, No. 5, February 3, 2015, pp. 169

et seq.; Dr.Moaz Suleiman Alma: The idea of the right to enter into digital limbo in modern electronic penal legislation; A comparative study between French penal legislation and Kuwaiti penal legislation, Journal of the Kuwait International Law College, Research of the Fifth International Annual Conference, May 9-10, 2018, Special Supplement, No. 3, Part One, May 2018, p. 117 and beyond.

- Hossam Muhammad Nabil Al-Shanraqi: Protection of Personal Data via the Internet: Challenges and Solutions, The Arab Journal of Management, Supplement, Issue Two, Volume 38, 2018, p.