ITJ | The International Tax Journal

Limits of processing personal data in digital transactions

Adel Lemouchi [1]

[1] Lecturer (A), Laboratory for Legal Studies and Research in Light of Major Dangers, Souk Ahras University, (Algeria). Email: a.lemouchi@univ-soukahras.dz

Abstract---Digital transactions are no longer confined to one field but have spread to almost all areas, and there is no escape from them. One of the requirements of these transactions is the necessity to declare personal data, which is referred to as digital privacy and is legally protected. However, this protection may not extend to data voluntarily provided by the individual involved in the transaction. Therefore, there is a need to establish regulations and limits for data collectors and processors that take into account the nature of the transaction, the purpose of processing, the principle of adequacy, and the necessity of digital forgetting.

Keywords---personal data, digital transactions, data aggregation, digital processing.

Introduction

Electronic transactions have become the most popular in the world of commerce due to their numerous advantages, especially speed and ease of procedures. Individuals and groups alike have no choice but to use them. Digital transactions have established themselves in all fields and have become the primary driver of transactions, regardless of their nature.

Digital transactions require the provision of any information relevant to the identity and character of the transaction. This personal data may be over looked by the transaction, as they believe it is futile. This may be the case, but with the endless development of digital transactions, this personal data has acquired value, both in the world of commerce due to the reputation it brings to the professional or supplier, and for various purposes depending on who collected the data, whether political, economic, etc.

Hence, the importance of studying this topic emerges. This study aims to shed light on the importance of personal data in the digital environment, as well as to understand the nature of this data based on the

How to Cite:
Lemouchi, A. (2025). Limits of processing personal data in digital transactions. *The International Tax Journal*, *52*(3), 805–813. Retrieved from https://internationaltaxjournal.online/index.php/itj/article/view/102

The International tax journal ISSN: 0097-7314 E-ISSN: 3066-2370 © 2025

Submitted: 07 Feb 2025 | Revised: 10 March 2025 | Accepted: 25 April 2025

nature of individuals, and to examine the mechanism for collecting and processing data according to the purposes intended by the collector. Legal protection for personal data in international law is enshrined in a framework that ensures that this data is surrounded by a wall that prevents tampering with it.
However, the boundaries of this wall are often controlled by the data processor based on the user's consent. The latter finds themselves subject to the supplier or business professional, providing their personal data below a certain limit. This exposes them to the use of this data, in excess of the purpose of the transaction, for purposes the requester seeks to achieve, with or without the knowledge of the user.

Based on the above and through stating the importance of the study, we pose the following question: "Given the privacy that personal data represents for the user, and his right to be surrounded by what guarantees its confidentiality, and to provide the minimum amount of it, what are the controls that the data collector and processor must take into account when dealing with data of a personal nature"?

To answer the question, I followed a descriptive approach to clarify the meanings of the research terms, along with a deductive approach to derive the relevant rulings that lead to answering the question. I divided my research into two axes: the first, processing personal data; and the second, data processing controls. First: Processing Personal Data
Before delving into the concept of personal data processing, it is necessary to address this data by defining it and listing its components. This will facilitate understanding the processing and the risks it poses to personal data.

A- The Concept of Personal Data:
The concept of information privacy is similar to the concept of personal data, although the latter is broader in scope and application and expands according to each individual. What is public to one person is private to another. Therefore, information privacy is part of personal data.

Definition of Personal Data:
It's important to note the need to distinguish between data and information. The former refers to the raw material of information, consisting of words, numbers, and symbols. It has no meaning in and of itself, and cannot be relied upon alone to understand a specific matter[1]. It is also a set of facts that express certain attitudes and actions, whether expressed in words or symbols. In reality, in the form we have mentioned, it is of no use[2]. Data, on the other hand, is defined as: data that has been processed and organized so that it can be exploited for specific purposes[3]...
While personal data is defined as information that identifies an individual, such as name, address, phone numbers, and marital status, all of which are characteristics of a person's personality[4], it's worth noting that there is a close relationship between data and information, although there is a difference between them. Information cannot exist without data, which is the raw material that can be processed to produce a more useful and usable form, information[5].

---

[1] EgyptAir Training Center, *Introductory Course on Data Processing*, June 2016, p. 2. Available at: https://training.egyptair.com/Catalog/Students
[2] Rabhi Aziza, *Information Secrets and Their Penal Protection*, PhD thesis in Private Law, Faculty of Law and Political Science, University of Abou Bekr Belkaid – Tlemcen, 2017/2018, p. 2.
[3] Haidar Hassan Mohammad, *Knowledge Management Strategies: An Analytical Study in Information Institutions in Iraq*, Arab Gate for Libraries and Information Organization, Issue 41, 2016, p. 07.
For further reading:
Mohammad Ali Fares Al-Zoghbi, *The Legal Protection of Databases According to Copyright Law: A Comparative Study Between the Latin and Anglo-American Systems*, Al-Maaref Establishment, Alexandria, 2003, pp. 76–77.
[4] Amin bin Salem Al-Harthi and Mohammad bin Saleh Al-Tuwaireqi, *Organization and Management of Personal Information*, 9th International Academic Scientific Conference titled *"Contemporary Trends in Social, Human, and Natural Sciences"*, held on July 17–18, 2018, Istanbul, Turkey.
[5] Jawhar Qouadri Samet, *Legal Regulations for Electronic Processing of Personal Data*, *Comparative Legal Studies Journal*, Hassiba Ben Bouali University, Chlef, Vol. 6, No. 2, 2020, pp. 469–470.

1- Definition of information privacy:
The term "the right to privacy" was first used in an article published in 1890 by Brandies Warren in the Harvard Law Review in the United States. It is a concept related to the individual's being or private space, through which they seek to protect their feelings, thoughts, and private secrets, embodying their individual being[6].

If we come to the contemporary technical meaning of the word privacy, in English it means: "The right of an individual to preserve his personal information and his private life, voluntarily and freely." The first privacy law was written by the American Louis Brandeis: "Privacy is often the ability of a person or a group of people to prevent information about him or them from becoming known to others, especially organizations and institutions, personal information, if the person does not voluntarily choose to provide that information." The term privacy, originally a concept that refers to the scope of private life, has evolved more broadly in recent decades, to include the right to control personally identifiable data[7].

Privacy is often associated with personal data. Jurisprudence has defined information privacy as: "The right of individuals, groups, and institutions to determine for themselves when, how, and to what extent their private information may be disclosed to others." UNESCO defines personal data as: "any information relating to a specific individual (the person concerned) that allows that person to be identified, either directly or indirectly, based on that data itself or through the taking of reasonable feasible measures, when UNESCO, or another party on its behalf, processes that data in the performance of its mandate. By "data processing," UNESCO means any operation or set of operations, whether automated or not, that handles personal data or sensitive non-personal data, including collection, storage, use, transmission, and erasure[8].

Another definition is: "the ability of an individual to control the handling of information concerning him." It is also defined as: "the right of an individual to regulate the collection, automated processing, storage, dissemination, and use of his personal data for decision-making purposes." It is also defined as: "the right of individuals, groups, or institutions to limit the extent to which information relating to their private lives is accessible to others, and to control the automated collection, processing, and use of personal data for decision-making purposes affecting their lives"[9].

Digital privacy is defined as: "the protection of users' data on the Internet. It is one of the rights that many relevant institutions are calling for the necessity of implementing so that users can browse the Internet without worrying about the possibility of their data being stolen and used, whether positively - targeting consumers to buy a specific product based on their preferences, interests, and the information they are searching for - or negatively - stealing that data to blackmail its owners for the purpose of obtaining money or even exploiting it by sovereign entities to direct voters or monitor certain individuals"[10].

2- Personal Data Elements:
2-1- Name Data: This is everything given to a person to distinguish them from others, whether it is a formal name, a nickname, or a pseudonym. This name data contributes to identifying the person.
2-2- Image: A person's image is considered personal data that allows for the direct identification of its owner, and every person enjoys legal protection for their image.

---

[6] Wasim Shafiq Al-Hajjar, *The Legal System of Social Media*, Arab Center for Legal and Judicial Research, Council of Arab Ministers of Justice, League of Arab States, 1st ed., Beirut, 2017, p. 37.
[7] Available at: https://2u.pw/zoZsQ5T
[8] Available at: https://www.unesco.org/ar/privacy-policy
[9] Hossam El-Din Al-Ahwai, *The Right to Respect for Private Life (The Right to Privacy): A Comparative Study*, Dar Al-Nahda Al-Arabiya, 2nd ed., 2002, p. 132.
[10] See: https://2u.pw/rxHd5

2-3- Personal Numbers: With the development of societies, people have become surrounded by numbers, such as the national ID number, telephone number, bank account number, and social security number. Through these numbers, the identity of their owner can be identified, as they are numbers specific to a specific person and are not repeated within a single country.
2-4- Personal Addresses: With the development of communication and information technology, people have come to know addresses other than their geographical address, such as email addresses, whether personal or professional, and Internet Protocol (IP) addresses.
2-5- Human biometrics: These are the vital and physiological characteristics and measures that a person possesses, which vary from person to person, including fingerprints, iris prints, voice prints, DNA fingerprints, and facial features. Modern science has developed technologies capable of processing and identifying these characteristics, then programming each person's characteristics, encrypting them, and storing them in an electronic database, allowing for rapid identification. Therefore, human biometrics are considered personal data, as they are non-repeatable.
2-6- Health status: This refers to a person's medical condition or medical history. This health status is considered personal data and may not be disclosed under any circumstances, even by the treating physician.
2-7- Political and union opinions: A person's political and union opinions are considered personal data, and the French National Commission for Informatics and Freedom prohibits the collection of this data without the written consent of the data subject.
2-8- Religious beliefs: Religious belief refers to a person's belief in a particular religion.
2-9- Nationality and ethnic origins: Nationality is a person's affiliation to a particular country, while ethnic origins are a person's affiliation to one of the human groups that are characterised by inherited genetic characteristics that distinguish them from other human groups.

A- Processing of Personal Data in the Digital Environment:
Although there is no unified definition in a global treaty, the definitions and principles found in international and regional legal frameworks provide a solid basis for understanding and regulating the processing of personal data at the international level.

1-The Concept of Personal Data Processing:
The science of rational processing, by automated means, of information.
According to Algerian Law No. 18-07 of June 10, 2018, relating to the protection of natural persons in the field of personal data processing, personal data processing is defined as: "Any operation or set of operations performed on personal data, whether automated or non-automated, specifically collecting, recording, storing, organizing, storing, adapting or modifying, retrieving, consulting, using, disclosing, transmitting, disseminating, or otherwise, approximating or linking them together, as well as restricting, erasing, or destroying them[11]".

In other words, this definition includes any activity carried out on data that identifies or makes a natural person identifiable, from the collection of such data to its destruction. The law aims to regulate these processes to ensure the protection of individuals' fundamental rights and freedoms, particularly with regard to their privacy. According to EU Regulation 2016-679 on the protection of individuals with regard to the processing of personal data, processing is defined as "any operation or set of operations, whether performed by automated means or not, applied to personal data or sets of data, such as collection, recording, organization, structuring, storage, adaptation or alteration, extraction, consultation, use, communication by transmission, dissemination or otherwise making available, approximation or interconnection, identification, erasure or destruction". From the aforementioned definition, we can derive the basic elements:

[11] Article 03 of Law No. 18-07 dated June 10, 2018, concerning the protection of natural persons in the field of processing personal data.

- Personal nature: Personal data relates to a natural person, whether identified or identifiable. Identification may be direct through a name, or indirect through a set of numbers, such as a national identification number; a personal or professional email address; an Internet Protocol (IP) address; or factors specific to the physical, physiological, genetic, or mental identity of the natural person.
- A process or set of processes: This includes any activity performed on the data, regardless of the means used (automated or manual).
- A broad range of activities: Processing covers a wide range of actions that can be taken with respect to the data, from initial collection to final destruction.

Article 1 of the African Union Convention on Cybersecurity and Personal Data Protection, paragraph 37, defines it as: "A process or set of processes performed on personal data with or without the aid of automated means, such as collecting, recording, organizing, storing, adapting, modifying, extracting, protecting, copying, consulting, using, disclosing through transmission, dissemination or any other form of making available by alignment, linking or blocking, as well as encrypting, deleting and destroying personal data." 2- Collection Mechanism:

Due to technological advancements, human activity has shifted from the physical world to the virtual world. The Internet was the space in which the transition and transformation towards digitization took place, and the latter added the largest mechanism for collecting personal data. Online stores seek to use several methods to intrude on this data. Among the most prominent intrusion techniques are:

2-1- Cookie Technology:

You often encounter the message that appears upon clicking on any website: "Do you agree to the use of cookies?" This message may seem annoying to you, but it means a lot to the website owners, as it allows them to monitor the user's experience, the length of time they spent on each page, and the duration of their browsing of the website as a whole. These cookies can be used for analytical and marketing purposes. These cookies do not store the user's name or data; they only store your device profile and your location on the map. This cookie technology relies on sending technical files called cookies from the store's server to the internet user's computer as soon as the latter visits the store's website. These files record the personal information the user entered on the websites they interact with. This technology then records all the user's traces on the websites they visited, including the time of the visit, length of stay, searches, product previews, purchase requests, and downloads.

2-2- Phishing Scans:

Some websites of an organization with which the user interacts, impersonating the identity of this organization, send the user an email containing a link to this fake website, then asking them to click on the link to update their personal information to avoid being suspended from the organization. When the user clicks on the link, the fake website asks them for their personal information. The store's goal in this process is usually to collect as much personal information as possible, to be used for its own benefit in advertising and marketing operations, or to sell it as other virtual stores.

Second: Data Processing Control (Methods or Means of Protection)

The issue of protecting the privacy of internet users is among the topics that present themselves for research and discussion. This has prompted many countries to issue laws related to protecting the privacy of individuals, particularly with regard to protecting their personal data, by establishing the necessary controls for processing this data.

Legislation has enacted a set of laws aimed at protecting privacy. However, these laws remain powerless in the face of the astonishing development of information technology. This is especially true since criminalization is linked to its most important component, namely the legal component. No person can be prosecuted unless there is a text criminalizing their act.

A- Risks of Data Processing and Methods of Protection

The reality is that the danger in this area lies in the fact that online stores collect the personal data of internet users, whether contractors or visitors, for the purpose of processing them and creating a database that can be used to serve the interests of the stores.

1- Risks of Data Processing

1-2- The internet's processing of the personal data of its suppliers poses a risk to this data due to the network not being owned by a specific entity or country, in addition to its open nature, which escapes control or surveillance due to intrusion.

1-2- Data collection can provide access to this data fraudulently or in an authorized manner. This facilitates the misuse of data, misdirection, monitoring of individuals' privacy, or judgment of them based on their data.

1-3- The possibility of retaining personal data for a long period of time is inconsistent with the right to digital oblivion, which contradicts the purpose of data processing.

1-4- Selling personal data to online stores, which use them for advertising and marketing, thus becoming a commodity traded for a fee.

1-5- The difficulty of internet users concealing their data.

2- Methods of Protecting Personal Data

These methods serve as a safeguard against fraudulent and data-related scams. These methods include:

2-1- Data security technology: This is a type of technology used to encrypt a set of information transmitted over the internet, limiting the ability to retrieve content to the sender and recipient only. This technology is combined with a third-party authentication system to confirm that the real customer is interacting with the site. Combining the two methods ensures the confidentiality of commercial transactions and secure pages. 2-2- Authentication certificates: These are encrypted files stored inside the WAP service device with the browser program used by the client, and are usually recorded by a third party. These files consult with the browser program used by the client to ensure that the site entered by the user is the correct site. This technology is also used to verify the identity of network users, whether they are from inside or outside, so the authentication certificate is like an electronic driver's license, passport, or certificate of good conduct.

Note: Data security technology or a certificate of authentication does not, in fact, prevent data processing. The former prevents any intrusion into encrypted transactions. The certificate of authentication helps verify the identity of internet users.

A- Personal Data Processing Control:

The necessity of dealing in the virtual world necessarily requires each user to provide their personal data, depending on the nature of the transaction. This helps verify their identity. The more accurate the data provided by the user, the more serious the transaction is. However, the problem arises in retaining and processing this data in a manner that serves the interests of the supplier or professional. Therefore, it is imperative to establish a processing control to ensure the completion of the transaction and guarantee the right to protect personal data.

1- The Principle of Prior Consent to Processing:

Personal data may only be processed with the explicit consent of the person concerned, who may withdraw it at any time. The process also specifies the cases in which processing is necessary, and therefore the consent of the person concerned is not required[12].

It should be noted that personal data subject to processing may only be disclosed to third parties to achieve purposes directly related to the duties of the data controller and the recipient, and with the prior consent of the data subject[13]. Accordingly, any processing carried out in the absence of such prior

[12] Article 7, Paragraph 5 of Law No. 18-07 dated June 10, 2018, concerning the protection of natural persons in the field of processing personal data, Official Gazette No. 34.

[13] Article 7, Paragraph 4 of Law No. 18-07, dated June 10, 2018.

consent is considered unlawful processing. This consent resolves any dispute that may arise between the data controller and the data subject, as the exercise of each of their rights and obligations depends on the data subject's response.

2- The principle of proportionality (the suitability of personal data for the purposes for which it was collected):

This principle requires that personal data be relevant, appropriate, and not excessive, given the purpose for which it was initially collected and subsequently processed. This principle requires that any processing be based on data directly related to the purposes initially defined for processing. The principle also requires that processing be not only feasible, but also necessary, as required by the nature of the transaction, while taking into account the principle of balancing the treatment and the necessity of processing without exaggeration[14].

The legitimate purpose of collecting personal data is to conclude and perform a contract. Processing personal data is legitimate if it is necessary and required to perform a contractual obligation, perform a legal act, or conclude a contract for the benefit of the data subject. Legislation also requires that the processor obtain written authorization from the data subject. Accordingly, data must be collected for specific, explicit, and legitimate purposes and may not be processed in a manner that conflicts with those purposes.

3- The principle of abandonment due to the expiration of the purpose (the principle of limited retention period):

The processor is obligated not to retain personal data after the purpose of processing has been fulfilled. It may be retained if the data subject's identity has been concealed using the "anonymization mechanism" feature. The implementing regulations may also add or impose processing controls as may be necessary and appropriate for the processing of personal data in light of the ongoing development of digital privacy[15].

According to this principle, personal data must be retained in a manner that identifies the persons concerned, for a period not exceeding the period necessary to achieve the purposes for which the data was collected and processed. The principle also requires that data not be permanently stored in automated files. The retention period must be determined temporarily based on the objectives associated with each file created, unless the data subject has given permission to retain the data for a period longer than required by the nature of the transaction. This should be taken into account for the legality of retention, such as for historical, statistical, or scientific purposes[16].

That is, the storage period must be limited, and data must be retained in a form that allows the data subject to be identified for a period no longer than necessary for the purposes for which it is processed.

4- The principle that processing must be fair, transparent, and lawful:

The processing of personal data must be lawful, fair, transparent, and just. This principle relates to all aspects of personal data processing, and processing is legally based as long as it complies with each of the conditions stipulated in the law and regulations.

The rules require the data controller to be able to verify and confirm the availability of these conditions before initiating any processing procedure. These conditions are the minimum requirements that must be met for the lawful processing of personal data. Processing is lawful if it is carried out with the data subject's consent, or if the processing is necessary for the conclusion or performance of a contract to which the data subject is a party, or if the processing is necessary for the performance of a legal

---

[14] Toumi Yahia, *The Legal Protection of Personal Data in Light of Law No. 18-07: An Analytical Study*, *Al-Ustadh Al-Bahith Journal for Legal and Political Studies*, Mohamed Boudiaf University, M'sila, Vol. 04, No. 02, 2019, p. 1535.

[15] Al-Saghir Mohamed Mehdi, *Ibid.*, p. 329.

[16] Toumi Yahia, *Op. cit.*, p. 1536.

obligation imposed on the controller, or for the protection of the vital interests of the data subject or another natural person, or for the performance of a task required by the public interest[17].

5- The Adequacy Principle:
This means that personal data should be sufficient and limited to what is necessary for the purpose for which it was processed. Some call this principle the rationalization of data processing, as laws and regulations require anyone processing personal data to collect the necessary and sufficient amount of personal data that is appropriate and related to the specific and precise purpose of the processing[18].
The previous European Directive stipulated that the data subject to processing should not be over-collected, which is an unspecified restriction. The restriction in the regulation requires the data controller and processor to not exceed the processing for its specific purposes. This is more specific and precise than the prohibition of over-processing, as the regulation specified the standard of relating the processing to the need or purpose for which it was processed. However, the prohibition of over-processing opens the door to interpretation regarding what is meant by excessive processing. The rationalization of data processing principle does not apply only to data collection, but to all stages and types of data processing. Data may be collected lawfully, but its subsequent uses may be unlawful. For example, if the purpose of the processing requires that it be accessed by a few people within the control of the controller or processor, it should not be made available to others. Requesting the disclosure of driver's license data for a job unrelated to driving a car violates this principle. Neither a data controller nor a data processor can claim that the data subject voluntarily provided their data to a selective question on a specific form they completed. Therefore, personal data processors are held liable whenever the minimum required for the transaction is exceeded, even if the user expressly consents to the additional disclosure, as this is evidence of fraud and deliberate intent on the part of the processor[19].

Conclusion:
Personal data takes on elements whose value depends on the purposes for which it was processed. Whatever the purpose, it has value in the ever-evolving digital world. This has led to increasing concerns about personal data. Therefore, it became necessary to establish controls for the collection and processing of personal data, to serve the interests of users and the processor, as transactions require.

From the above, we reached the following conclusions:
1. Personal data is everything that identifies and relates to a person, whether by name, title, or appearance. Despite its diversity, it has value in electronic transactions, regardless of the person's value.
1. Personal data is linked to digital privacy and represents a legal ownership right. Financial transactions are subject to it when the data subject consents to the marketing of the data, such as product promotions or a survey on a particular trend.
2- The processing and collection of personal data and the right to digital privacy are two equations that must be reconciled without favoring either party. Favoring any party would either disrupt digital transactions by overprotecting personal data or jeopardize privacy in the digital environment.
3- The data processor has no legal liability if it observes the processing limits and controls as required by the transaction. Its liability remains with respect to the data it requests that are not related to or required by the transaction.
4- The digital oblivion of personal data requires that data not be retained for a period inconsistent with the nature of the transaction and the right to digital privacy.

---

[17] Al-Saghir Mohamed Mehdi, *The Legal Nature of Digital Privacy: A Study to Clarify the Provisions Governing the Protection of Personal Data Through Digital Technology*, Conference on Legal Challenges in the Digital Age, 8th Scientific Conference of the College of Law, Sultan Qaboos University, 2024, pp. 326–327.
[18] Al-Saghir Mohamed Mehdi, *Op. cit.*, p. 327.
[19] Regulation (EU) 2016/679 issued by the European Parliament and Council on April 27, 2016, concerning the protection of natural persons with regard to the processing of personal data and the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text relevant to the European Economic Area).

5- Both national and international legislation remain unable to keep pace with the developments taking place in the digital environment, which necessitates adapting to this development in a manner that is appropriate and appropriate for the preservation of personal data.

Inspired by these findings, the following proposals were made:

1- The need to expedite the development of legal rules with an international character, given that the digital environment does not recognize borders. Therefore, the protection of personal data is an international, not a national, requirement.

2- The need to create specialized courts in countries to hear disputes over digital privacy and artificial intelligence. This requires a qualified human element to preserve the rights of professionals and users alike.

3- Raising awareness among digital users of the right to digital privacy, the need to review privacy policies and terms of use, and educating them about the importance of adjusting privacy settings.

Bibliography:

[1] Law No. 18-07 dated June 10, 2018, concerning the protection of natural persons in the field of processing personal data, Official Gazette No. 34.

[2] Hossam El-Din Al-Ahwai, The Right to Respect for Private Life (The Right to Privacy): A Comparative Study, Dar Al-Nahda Al-Arabiya, 2nd ed., 2002.

[3] Mohammad Ali Fares Al-Zoghbi, The Legal Protection of Databases According to Copyright Law: A Comparative Study Between the Latin and Anglo-American Systems, Al-Maaref Establishment, Alexandria, 2003.

[4] Wasim Shafiq Al-Hajjar, The Legal System of Social Media, Arab Center for Legal and Judicial Research, Council of Arab Ministers of Justice, League of Arab States, 1st ed., Beirut, 2017.

[5] Rabhi Aziza, Information Secrets and Their Penal Protection, PhD thesis in Private Law, Faculty of Law and Political Science, University of Abou Bekr Belkaid – Tlemcen, 2017/2018.

[6] Toumi Yahia, The Legal Protection of Personal Data in Light of Law No. 18-07: An Analytical Study, Al-Ustadh Al-Bahith Journal for Legal and Political Studies, Mohamed Boudiaf University, M'sila, Vol. 4, No. 2, 2019.

[7] Jawhar Qouadri Samet, Legal Regulations for Electronic Processing of Personal Data, Comparative Legal Studies Journal, Hassiba Ben Bouali University, Chlef, Vol. 6, No. 2, 2020.

[8] Haidar Hassan Mohammad, Knowledge Management Strategies: An Analytical Study in Information Institutions in Iraq, Arab Gate for Libraries and Information Organization, Issue 41, 2016.

[9] Al-Saghir Mohamed Mehdi, The Legal Nature of Digital Privacy: A Study to Clarify the Provisions Governing the Protection of Personal Data Through Digital Technology, Conference on Legal Challenges in the Digital Age, 8th Scientific Conference of the College of Law, Sultan Qaboos University, 2024.

[10] Amin bin Salem Al-Harthi, Mohammad bin Saleh Al-Tuwaireqi, Organization and Management of Personal Information, 9th International Academic Scientific Conference titled "Contemporary Trends in Social, Human, and Natural Sciences," held on July 17-18, 2018, Istanbul, Turkey.

Websites:

[1] https://2u.pw/BCDzf

[2] https://2u.pw/BCDzf

[3] https://www.unesco.org/ar/privacy-policy

[4] EgyptAir Training Center, Introductory Course on Data Processing, June 2016, p. 2, available at: https://training.egyptair.com/Catalog/Students.