مجلة الدراسات القانونية المقارنة
EISSN:2600-6154 المجلد09/ العـــدد02 (2024)، ص.ص.208-225 ISSN:2478-0022

Governance of Personal Data Privacy in Algerian Legislation

حوكمة خصوصية المعطيات الشخصية في التشريع الجزائري

د. بن قارة مصطفى عائشة

Aicha BENKARAMOSTEFA

أستاذة محاضرة قسم "أ"، التخصص: (القانون – قانون عام)، كلية الحقوق والعلوم السياسية جامعة مستغانم، الجزائر.

Lecturer-A-, Specialization: (Law, public Law), faculty of Law and Political Sciences, University of mostaganem

aicha.benkaramostefa@univ-mosta.dz

تاريخ إرسال المقال:2024/01/23 تاريخ القبول:2024/03/18 تاريخ النشر:2024/03/29

ملخص:

في ظل ما للمعطيات الشخصية في عصرنا الحاضر من أهمية، أصبحت تحظى باهتمام خصوصا في ظل خضوعها لنظام تحكم مركزي للإدارة العمومية، مما أثار تخوفات شديدة على حماية الشخصية، الأمر الذي تطلب تدخل تشريعي كانت بداياته من التعديل الدستوري لسنة 2016 حيث أدرج هذا المفهوم لأول مرة في الدستور مرورا بالقانون رقم 18-07 المتعلق بحماية الأشخاص الطبيعيين في مجال معالجة المعطيات ذات الطابع الشخصي، يأتي هذا القانون لحماية الكرامة الانسانية والحياة الخاصة أثناء المعالجة الألية للمعطيات الشخصية من قبل المؤسسات العمومية أو الخواص من خلال احترام مبادئ حوكمة المعطيات الشخصية. وبهدف تثمين المنظومة القانونية في مجال حماية المعطيات الشخصية وتحيينها يمكن اقتراح ضرورة وعي الأفراد نحو بياناتهم الشخصية وتنبيههم بالمخاطر التي تحيط بها، إقرار مدونات قواعد السلوك في مجال حماية البيانات الشخصية يقتاد بها الموظفين التابعين للجهات المسؤولة عن معالجة المعطيات الشخصية.

كلمات مفتاحية:

المعطيات الشخصية، السلطة الوطنية، المعالجة الآلية، الحوكمة، الخصوصية المعلوماتية.

Abstract:

In the present era, personal data has become increasingly important, especially as it is subject to a centralized control system by the public administration. This has raised serious concerns about the protection of privacy, which has required legislative intervention. This intervention began with the constitutional amendment of 2016, which included this concept for the first time in the constitution. It continued with Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data. This law aims to protect human dignity and privacy during the

L'auteur: BENKARA MOSTEFA Aicha **Email:**aicha.benkaramostefa@univ-mosta.dz

automated processing of personal data by public or private institutions through the respect of the principles of personal data governance. In order to enhance the legal system in the field of personal data protection and to update it, it is proposed to raise awareness among individuals about their personal data and warn them of the risks associated with it , and adopt codes of conduct in the field of personal data protection, which employees of entities responsible for processing personal data are required to follow.

Keywords:
Personal data, national authority, automated processing, governance, information privacy

Introduction:

There is no doubt that the development of modern information and communication technologies and their widespread use has led to the possibility of collecting, storing, and processing data, whether by public institutions or the private sector. This has made data a primary commodity in many fields, and the internet has facilitated the flow and exchange of this information between different countries around the world. This has led to a growing awareness of the risks of technology and its threat to privacy through the misuse of personal data, which may contain information about a person's personal life, such as their health status, financial activities, and political opinions. All of this poses a threat to privacy.

This has motivated international, regional, and national efforts to find principles and rules that would protect the right to privacy and, by necessity, find a balance between the needs of society to collect, store, and process personal data and ensure the protection of this data from the risks of misuse of the technologies used to process it.

Therefore, personal data and electronic processing have become of great importance at the international level, as enshrined in Article 12 of the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights of 1966. This led the United Nations to adopt in 1989 a guide on the use of personal data in the flow of data, and on 14 December 1990, the General Assembly adopted a guide on the regulation of the use of automated processing of personal data.

The Organization for Economic Cooperation and Development (**OECD**) also began in 1978 to develop guidelines and codes of practice on privacy protection and data transfer. In addition, the European Union has issued guidelines on data protection, the most prominent of which is the 1995 guide on the protection of individuals with regard to the processing of personal data and the free movement of such data, as well as the 1997 guide on the protection of telecommunications data.

As for national legislation, Sweden was the first country to adopt a protective framework through the Data Protection Act of 11 May 1973, as well as a new legislative framework in 1998. In the same vein, France issued Law No. 77-78 on Informatics, Files, and Freedoms on 6 January 1978, which was amended in 2004.

As for Arab countries, Tunisia is considered to be the first Arab country to establish a protective system that is compatible with European Union directives through the Fundamental Law No. 63 of 24 July 2004 on the Protection of Personal Data. This was followed by the United Arab Emirates through the Personal Data Protection Law of 2007 No. 1, which is specific to the Dubai International Financial Centre (DIFC). Oman followed with Sultani Decree No. 2008-69 in the context of the Electronic Transactions Law. Morocco issued Law No. 09-09 of 2009 on the Protection of Natural Persons with Regard to the Processing of Personal Data.

In the face of attacks that threaten privacy, as well as international attention, the concept of personal data began to find its place in Algerian legal texts, starting with the constitutional amendment of 2016 (Law, 16-01; 2016). This concept was included in the Constitution for the first time by adding the fourth paragraph of Article 46, which states that "the protection of natural persons in the field of processing personal data is a fundamental right guaranteed by law and punishable for its violation."

Therefore, the preservation of the privacy of personal data, as a civilized concept and an individual demand, requires the regulation of its handling and governance as one of the state's strategic priorities. This is done through Law No. 18-07 on the Protection of Natural Persons in the Field of Processing Personal Data (Article (43) Law No18-07, 2018), which is the legislative framework governing matters related to the protection of personal data.

Therefore, the research on the subject of personal data governance raises a central issue **: what are the rules and principles that the Algerian legislator has enshrined for the governance of personal data through Law No. 18-07 on the Protection of Natural Persons in the Field of Processing Personal Data with a Personal Character?**

This study required the use of the descriptive-analytical approach, which is based primarily on the rule of accurate description and in-depth analysis of data, to show their adequacy or inadequacy, in order to find the appropriate solution in solving and processing each of the elements that we will address.

In order to properly address this topic, we divided the research as follows:

Section One : The nature of personal data governance

Subsection One : Defining personal data

Subsection Two: The justifications for personal data governance

Section Two: The legal controls for personal data governance

Subsection One : Conditions for processing personal data

Subsection Two: The rights of the concerned person and the obligations of the data processing.

Section One : The nature of personal data governance

With the steady development in technology and the ease of obtaining and sharing data, the importance of maintaining the privacy of personal data is multiplying, which prompted most countries to enact regulations and legislation that regulate the collection, processing and sharing of personal data in a way that ensures the preservation of the privacy of the owners of this data and the protection of their

rights, and the governance of this data is important in maintaining national digital sovereignty over this data, through transparency and accountability for unethical behaviors Personal data.

Law No. 18-07 on the Protection of Natural Persons in the Field of Processing Personal Data with a Personal Character is an important tool in protecting the privacy and personal data of the Algerian citizen.and the legislator has explicitly clarified this in Article 2 of this law, which states: "The processing of personal data, regardless of its source or form, must be carried out in a manner that respects human dignity, privacy, and public freedoms, and must not infringe on the rights, honor, and reputation of individuals." Therefore, we will try to clarify the concept of personal data governance by explaining the meaning of personal data (first), and then explaining the justifications and reasons for resorting to personal data governance (second).

1. Definition of personal data:

Personal data has evolved with the development of the Internet, no longer available name, surname and postal address, but has increased and diversified to include a person's image and voice, in addition to another set of data related to his ability (financial), behaviors, habits, tendencies and tastes, and most of all data related to the human body "biometric data" (Ben Qara, 2016).

Therefore, does all personal data undergo automatic processing**?**

For automated processing? Are there exceptions to personal data protected by law?

1.1 Content of the definition

The Algerian legislator defined personal data through the second paragraph of Article (3) of the aforementioned Law No. 18-07, which stipulates that: "Personal data are any information, regardless of its support, related to a person identified or identifiable and referred to below as "the person concerned", directly or indirectly, in particular by reference to the identification number or one or more elements of his physical, physiological, genetic, biometric, psychological or economic identity. or cultural or social (Article (43) Law No18-07, 2018).

It is noticeable that the Algerian legislator expanded its definition of personal data, and did well to include data any information that can identify any person directly or indirectly, because the narrowing of the concept of personal data may allow many parties to infringe on it, especially with the advancement of data collection and sharing techniques, the data distributed in different databases may not indicate the identity of the person itself, but if it is linked, it may reveal the identity of the person, and this broad definition The flexible allows this law to be applied to any recent form of personal data that may appear in the future. In order to clarify this, we should indicate the scope of the data protected, and the processes of processing.

First: Scope of the definition of data

The definition of personal data established by the Algerian legislator is characterized by two characteristics: it requires that personal data relate only to natural persons and that they be able to identify the person to whom they relate.

(a) Personal data relates to a natural person:

Article 1/1 of Law 18-07 explicitly reaffirmed what is stated in the title of this law that personal data must relate to a natural person, which is also confirmed by the European Directive 95/46 of October 24, 1995 in Article 2/a thereof. Most European legislations, such as French, Belgian, and Dutch legislation, followed the same trend. However, some other legislations extended the scope of protection to legal persons, including Norwegian, Austrian, Irish, and Danish law (Tanuary, 1974, p. 10).

As for jurisprudence, most probable trend is that the scope of the Personal Data Protection Law should be limited to natural persons, since the protection of personal data is tantamount to protecting the right to private life, which is one of the rights related to the human personality.grounds that the protection of personal data is a form of protection of the right to privacy, which is considered one of the human personality rights (Tanuary, 1974, p. 15).

(b) The data enable the identification of a natural person:

In order for certain data to acquire a personal nature, it is necessary to identify the person to whom it relates. Referring to the definition provided in Article 3, paragraph 2 (3/2) of Law No. 18-07, it is clear that it is not necessary for the person concerned to be identified by name, postal address or photograph in a direct manner, but can be identified by indirect data that may determine his identity, such as personal data on the internet, including: cookie technologies, and Internet protocol ,the latter means (IP address) , which is the set of rules governing the format of data sent via the internet or local network.

IP is an address used for computing devices, such as personal computers, tablets, and smartphones. Its purpose is to assign an address to these devices so that they can communicate with other devices on an IP network. Each device has a unique IP address that is different from all other devices. (Al-Maqata, 1992, p. 123).

These elements constitute personal data if they enable the identification of a natural person, directly or indirectly The elements that enable identification of a person remain varied. They include all the elements specific to a particular person, as long as they are distinctive of his physical, physiological, genetic, biometric, psychological, economic, psychological, cultural or social identity.

Secondly, the definition of the processing of personal data

In order for personal data to be protected by Law No. 18-07, it must be treated, and Article three in its fourth paragraph (3/4) of the aforementioned law defines the processing of personal data: " Any operation or set of operations performed in ways or by automated means or without such data of a personal nature as collection, registration, organization, preservation, appropriate, change, extraction, access, use, delivery through transmission, dissemination or any other form of availability, approximation, interconnection, closure, encryption, survey or damage**".**

Through this definition, it is clear that data processing must be carried out through a process or set of processes, and that it must lead to the formation of a file of personal data.

1.2 Domain of application of legal protection of personal data

Personal data knows a striking variety, After the collection, storage, and use of this data was done manually using paper supports, this processing began to be done by mechanical means, especially after the advent of the computer. Many entities now create files related to personal data. After the collection, storage, and use of this data was done manually using paper supports, this processing began to be done by mechanical means, especially after the advent of the computer. Many entities now create files related to personal data. either in the public sector by administrations, public institutions, and local communities that have a set of files containing personal data (Data related to civil status, social security, electoral lists, etc.), as well as public hospitals that collect medical information and personal data of the individual within the "Your Health" project related to the digitization of the health sector, which aims in particular to improve the service provided to the citizen.

The Algerian legislator has restricted the scope of application of this law, by excluding in Article 6 of Law 18-07 some types of processing, and limiting them to three cases:

a) Personal data processed by a natural person for purposes that do not exceed personal or family use, provided that they are not transmitted to others or published.
b) Personal data obtained and processed in the interests of national defense and security
c) Personal data collected and processed for the purposes of preventing crimes, prosecuting their perpetrators, and suppressing them, and those contained in judicial databases that are subject to the text that established them and to the provisions of Article 10 of this law.

2. Justifications for data governance:

There are many justifications for the use of data governance as an effective way to control the processing of personal data. Before discussing these justifications, it was necessary to define the concept of data governance, and then to state the reasons for personal data governance.

2. 1 Concept of data governance

We will first discuss the concept of governance in general and data governance, then the principles on which data governance is based, as follows:

First - Definition of Data Governance

The term governance is a shortened translation of the term **GOVERNANCE CORPORATE**. The scientific translation of this term, which is agreed upon, is: "The style of exercising prudent management powers."

The definitions of this term have varied, so that each term indicates the point of view that the author of this definition adopts. The International Finance Corporation **(IFC)** defines governance as: "The system through which companies are managed and controlled. (Freeland, 2007, p. 23)"

The Organization for Economic Co-operation and Development **(OECD)** defines it as : "A set of relationships between the company's management, the board of directors, shareholders and other stakeholders. (Freeland, 2007, p. 24)"

In other words, governance means the system, i.e. the existence of systems that govern the relationships between the essential parties that affect performance, as well as the components that strengthen the institution in the long term and determine the responsible and responsibility.

The concept of governance has been introduced in several fields, including the protection of human rights and private freedoms. Therefore, this term has been used to manage personal data during processing, whether it is mechanical or manual.

Therefore, data governance can be defined as a set of practices and procedures that help to ensure the management of data, starting with the development of a data management plan and the development of controls and policies, up to implementation and compliance. This is achieved through a governance framework that clarifies the roles and responsibilities of stakeholders.

Data governance rules seek to achieve several objectives, including:

-Maintaining data sources, updating them, organizing them, and making them available only to permitted persons.

-Putting in place the necessary procedures for handling sensitive data to reduce unauthorized access.

-Protecting data from cyber attacks and security threats.

-Reducing potential risks and enhancing performance and efficiency.

-Ensuring transparency and accountability when using data.

Secondly: Principles of personal data governance

Data governance is defined as a set of practices and procedures that prioritize, organize, and apply policies around data, while following different regulations and limiting bad data practices. Therefore, data governance is essentially a part of data management, which in turn relies on key principles that are mandatory considerations in protecting personal data. These principles are (Principles of United Nations System Organizations on Personal Data Protection and Privacy, UNESCO. 2018):

- **Data confidentiality:** Personal data should be treated with due confidentiality.
- **Limited storage and purpose:** When storing personal data, it should not be stored for a longer period than is necessary to carry out the purpose for which it was processed. Personal data should also not be processed for purposes other than those for which it was collected.
- **Transparency:** Personal data should be processed in a transparent and clear manner for the individuals concerned, as appropriate and as far as possible. This includes, for example, providing information to the individuals concerned about the processing of their personal data and about how to request access to that personal data, verify it, and/or delete it, as long as those matters do not prevent the achievement of the specific purposes of the processing of personal data.
- **Data security and protection :** These are some of the procedures, techniques, and technical solutions needed to protect data from unauthorized access, modification, or deletion, as well as from electronic intrusions. They

clarify the steps that must be taken when dealing electronically with this data, in order to ensure the minimization of risks.

- **Accountability:** The need to follow the procedures that regulate the processing of personal data in a way that ensures the protection of the privacy of the owners of this data and the protection of their rights, otherwise the person responsible for the processing will be subject to legal action.

2.2Reasons for data governance

Despite the many benefits of information technology and global information networks, they have also created many risks, such as the ability to collect, store, and use information illegally without the knowledge of the owner. This is what we will try to explain below:

First - the computer and its relationship to the attack on informational privacy

The computer is a "device that performs arithmetic and logical operations for the instructions given to it at a very fast speed of up to tens of millions of arithmetic operations per second, and it also has the ability to handle a large amount of data with the ability to store and retrieve this data when needed."

Based on this, the use of computers by institutions, departments, government agencies, and private companies in the field of collecting and processing personal data has become possible, thanks to the cheapness of computing. However, this positive role of computers has left negative effects (Fikry., 2007, p. 645), which are represented in:

a) The possibility of making the chances of accessing this data illegally by means of fraud more than before, and opens up a wider field for misuse or misguidance.
b) The emergence of what is known as "information banks", where all countries of the world with their various institutions have turned to establishing databases to organize their work, and since personal information that was isolated and scattered, difficult to reach, has become in information banks, it is available and available more than before for use in purpoضases of surveillance of individuals.
c) The integration between information technology, communications, and multimedia has provided advanced audio, visual, and readable surveillance tools, in addition to software for tracking and collecting information automatically.

Secondly : The internet and its relationship to the attack on personal data

The internet is defined as "a network consisting of many computers connected to each other either by wired or wireless communication and extending to cover large areas of the globe." (Baqi, 2001, p. 4)

The internet provides many services in the field of obtaining information in various fields of life, it is a treasure trove of knowledge and a flowing stream of information.

If it has this importance, it is also a high-level tool for committing crimes, where electronically processed information is subject to espionage, theft, and manipulation with the intention of obtaining money or services that are not due, as browsing and surfing the internet leaves a large amount of information with the site owner, which is represented in the following (Jabri., 2005, p. 196):

1. IP address of the customer (IP), which can be used to identify the domain name and, accordingly, the name of the company or entity that registered the domain through the organization name domain and identify its location. (Eoghan Casey, 2004, p. 87)
2. Basic information about the browser, operating system, and physical system equipment used by the customer.
3. Time and date of the site visit.
4. Internet sites and the address of the previous pages that the user visited before entering the page in each visit.
5. It may also include information about the search engine used by the user to access the page, and depending on the type of browser, the user's email address may appear.

The privacy of others may be invaded using virus programs such as Trojan horses, worms, and logic bombs, or other technical means such as cookies and other programs.

Among the risks of the internet is the hacking or unauthorized entry by hackers, or the illegal stay in a private communication system, and the collection of private information about others, through intelligent software that is sent in emails, or through appearing as fake links that can spy on the user, or even commit other crimes such as cyber theft and fraud.

It is clear from the above that there are new challenges posed by the internet in the face of protecting informational privacy, as it has increased the volume of data collected and processed and has enabled the globalization of information, and thus the loss of centralization and control mechanisms.

Third: The impact of artificial intelligence systems on personal data:

In the midst of the implications of the Fourth Industrial Revolution and its great growth in the application of artificial intelligence in the service of humanity, which has affected many areas of human beings, from trade, industry, medicine, education, agriculture, and home services, but it can be a source of many risks that man did not know before and that could threaten his private life.

It is known that the neural axis of artificial intelligence necessarily depends on the database that is available to this intelligence, the more this base expands, the deeper the concept of intelligence becomes in it and becomes more precise and effective in performing the desired goals, as long as the data is characterized by generality, no legal problem is raised, but the problem arises with regard to private data.

This is because artificial intelligence in its civil or commercial dimension depends on a huge database about the people it deals with, in terms of names,

professions, work, gender, health status, family history, social security numbers, bank account numbers, and other information, which may fall under the concept of protected personal data in accordance with the European definition of the concept of personal data, in terms of being information that relates to an identified or identifiable natural person, directly or indirectly, by reference to an identifier or to one or more of its identification elements (Muhammad, 2020). The following are some of the privacy challenges of artificial intelligence :

-Data that is collected about people who are not the targets of the data collection process.

-The existence of data for a longer period of time than the people who created it, as a result of the decline in the cost of data storage.

-The use of data beyond the original purpose for which it was collected.

-Data collection based on artificial intelligence raises the debate about privacy issues, such as informed consent, voluntary participation, and the ability of a person to withdraw freely.

The Personal Data Protection Law No. 18-07 includes a set of concepts related to personal data and processing methods that were studied in this section. Given the importance of this data as it represents part of the right to privacy for individuals, Law 18-07 came to strengthen the legislative system in Algeria by establishing basic rules for the governance of personal data, which is the subject of study in the second part of the research.

Section two : Legal controls for data governance

The Algerian legislator has established, through Law No. 18-07 on the Protection of Personal Data Processing, whether this processing is carried out by mechanical or manual methods, a set of foundations that represent the rules of data governance. These rules ensure that the processing of personal data protects the right of individuals to protect their privacy. These controls are first represented in the procedures prior to the processing process, and secondly in the set of rights enjoyed by the data subject on the one hand, and the obligations that fall on the person responsible for the processing on the other hand.

1-Conditions for the processing of personal data:

The conditions for processing personal data are divided between pre-processing procedures, consisting of obtaining prior authorization or license from the National Authority, and essential procedures related to the processing process itself, which involve obtaining prior consent from the data subject, and conditions related to the personal data to be processed. These obligations are described in detail below.

1.1 Prior procedures for processing

The Algerian legislator, in Article 12 of Law No. 18-07, above mentioned, required the prior authorization from the National Authority or a license before carrying out any personal data processing operation.

First - Obtaining prior authorization: Based on Article 13 of Law No. 18-07, the data responsible is required to file the prior authorization with the National Authority, which includes the commitment to carry out the processing in accordance

with the provisions required by the law, whether it is submitted in the traditional way by being present in person, or through email. In return, the National Authority must issue a receipt of deposit or send it electronically, immediately or within a maximum period of 48 hours. The permit is therefore provided prior to each processing of personal data with one purpose or one purpose associated with a single permit (Article (43) Law No18-07, 2018).

Two types of prior authorizations can be distinguished:

A. Ordinary authorization: This is the ordinary type of authorization, which is the general rule, and must include the data mentioned in Article 14 of Law No. 18-07. These data are as follows:

- Name and address of the data controller, and if applicable, the name and address of its representative.
- Nature of the processing, its characteristics, and the purpose or purposes intended.
- Description of the category or categories of data subjects and the data or categories of personal data related to them.
- Recipients or categories of recipients to whom the data may be sent.
- Nature of the data intended to be sent to foreign countries.
- Duration of data retention.
- Interest in which the data subject can, if applicable, exercise the rights granted to him under the provisions of this law, as well as the procedures taken to facilitate the exercise of these rights.
- A general description that can be used to make a preliminary assessment of the adequacy of the measures taken to ensure the confidentiality and security of the processing.
- Cross-linking or any other forms of approximation between the data, as well as the transfer to third parties or processing by subcontractors, in any form, whether free or paid.

In addition, the National Authority must be notified immediately of any change in the information mentioned above, or of any deletion that affects the processing. In the event of the transfer of a data file, the transferor is required to complete the authorization procedures provided for in this law.

In conclusion, the two types of prior authorizations are designed to ensure that the processing is carried out in a lawful and transparent manner. By complying with these procedures, data controllers can help to protect the rights of individuals to protect their privacy.

B ;Simplified declaration: Article 15 of Law 18-07 specifies two types of processing for which a simplified declaration is required:

The first type: Processing of personal data that is not likely to harm the rights, freedoms, and private lives of individuals.

The second type: Certain non-automated processing of personal data.

The authority responsible for determining the list of processing in both of these types is the National Authority.

Exemptions from the declaration requirement: While the declarations mentioned above, in both their ordinary and simplified forms, are mandatory for the data controller before any processing, there are cases in which the declaration requirement is not mandatory. These cases are related to the processing whose purpose is only to keep an open record that is accessible to the public or to any person who proves that they have a legitimate interest in doing so. This is explicitly stated in Article 16 of Law 18-07. However, in these cases, a data controller must be appointed, and their identity must be disclosed to the public and reported to the National Authority. The data controller is responsible for applying the provisions relating to the rights of individuals as provided for in this law.

In addition, the data controller who is exempt from declaration must provide any person who requests it with the information relating to the purpose of the processing, the identity of the controller, their address, the data being processed, and the recipients of the data.

Secondly, obtaining prior authorization: The Algerian legislator, in Article 17 of Law No. 18-07, required prior authorization from the National Commission when it becomes clear to it, upon studying the declaration submitted to it, that the processing to be carried out includes obvious risks to the respect and protection of the private life, freedoms, and fundamental rights of individuals.**

Therefore, as a general rule, the Algerian legislator did not specify, on an exhaustive basis, the cases in which it is required to obtain authorization to carry out the processing, as did the Moroccan legislator in Article 12 of Law No. 08-09 on the protection of natural persons with regard to the processing of personal data. Rather, it left the discretionary power to the National Commission to assess the extent to which the risk is present in the processing of personal data or not. In contrast, it mentioned some cases, by way of example, in which licenses are granted to data controllers before processing this type of data, as follows (Zarrouk., 2013, p. 82):

a) **Sensitive data:**

According to the definition provided by Article 3, paragraph 7 of Law No. 18-07, sensitive data are defined as:

Personal data that reveals the racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership of the person concerned, or that is related to their health, including their genetic data (Article (43) Law No18-07, 2018).

In principle, the processing of this type of data is strictly prohibited. However, it is possible to process sensitive data after obtaining a license for reasons related to the public interest and are necessary to ensure the exercise of the legal or regulatory tasks of the data controller, or when the processing is carried out with the explicit consent of the person concerned, in the case of a legal provision that provides for it, or with the authorization of the National Authority .

b) Linking of files belonging to one or more legal persons running a public service for different purposes related to the public interest:

The linking of files is here defined as a form of processing that consists of establishing a link between data processed for a specific purpose with other data held by another data controller or controllers, or held by the same data controller for the same purpose or for other purposes. Therefore, even for the linking process to take place, a license from the National Authority is required.

Therefore, the license application must include the information mentioned in Article 14 of this law. The National Authority must also make its decision within two (2) months of being notified. This period may be extended for the same period by a reasoned decision of its president. Failure of the National Authority to reply within the period mentioned in this article shall be considered a rejection of the application.

1.2. Procedures relating to the processing process itself

These procedures consist of the consent of the data subject to the processing of their personal data, in addition to conditions relating to the data to be processed by the data controller.

First, the consent of the data subject to the processing

In principle, personal data may only be processed if the data subject has expressed their explicit consent, in accordance with the provisions of Article 7 of Law No. 18-07. If the data subject is an adult or a minor, the consent is subject to the rules set out in the general law.

This is the general rule, but there are exceptions where the legislator considers that consent is not required to carry out the processing. These exceptions are specifically defined in Article 7, paragraph 5 (Article 7/5), which requires the processing to be necessary:

- To comply with a legal obligation on the part of the data subject or the data controller.
- To protect the life of the data subject.
- To perform a contract to which the data subject is a party or to carry out pre-contractual procedures taken at their request.
- To protect the vital interests of the data subject, if they are unable to express their consent from a physical or legal point of view.
- To carry out a task that is part of the public interest or within the exercise of public authority duties that the data controller or the person to whom the data is disclosed is responsible for.
- To achieve a legitimate interest of the data controller or the recipient, taking into account the interest of the data subject and/or their fundamental rights and freedoms.

Secondly, conditions relating to the personal data themselves:

The personal data to be processed by the data controller, whether public or private, must meet the following conditions:

-Personal data must be processed in a lawful and fair manner, collected for specific, explicit, and legitimate purposes, adequate, relevant and not excessive,

accurate and up-to-date, and kept for no longer than necessary for the purposes for which they were collected or processed.

2-The rights of the person concerned and the obligations of the handler:

The Law on the Protection of Personal Data in Algeria guarantees certain protection of such data by granting certain rights to the persons concerned and the obligation to deal with certain obligations.

2.1 Rights of the data subject with regard to the processing of personal data

The data subject who has their personal data processed is entitled to a set of rights and guarantees that provide them with the necessary protection. The Algerian legislator addressed these rights in Chapter IV, Articles 32 to 37, as follows:

First, the right to information :

Pursuant to article 5 of the aforementioned Act No. 18-07, the person being contacted must be informed of a set of elements. unequivocal information ", before this compilation is made, and the media must be unequivocal And this information is the responsibility of everyone responsible for processing or their representative, Only in the case where the person concerned is aware in advance of the elements to be informed of, these elements are: The identity of the processing officer and, where appropriate, the identity of his representative, for the purposes of processing, any additional useful information, in particular the addressee, the compulsory response, the implications, his rights and the transfer of data to a foreign country.

Article 33 of the same law excludes from the scope of the right to information a series of cases, exclusively where the person concerned is not entitled to inform. These include:

The first case is for personal data compiled for statistical, historical or scientific purposes,

The second case is if processed pursuant to a statutory provision, in which the legislative texts expressly provide for the registration or transmission of personal data as Electronic case law newspaper

The third case is processed exclusively for journalistic, artistic or literary purposes.

Secondly, the right of access:

The Algerian legislator has granted the data subject the right of access, in accordance with Article 24 of Law No. 18-07 mentioned above. The right of access is exercised by the data subject being summoned to review their file or read what is on the computer screen, depending on the circumstances.

It is noted that the legislator did not specify the practical procedures that could guarantee the application of this right so that it does not remain absent from practical practice, which is what the Moroccan legislator did, for example, by issuing the Implementing Decree of the Law on the Protection of Natural Persons with regard to the Processing of Personal Data No. 08-09.

Third, the right to rectification :

The data subject has the right to rectify personal data that is being processed by the data controller, as expressly stipulated in Article 35 of Law No. 18-07. This right

is a fundamental guarantee in monitoring the various processing that is carried out by them on personal data.

The person concerned has the right to obtain from the data controller, free of charge, the updating, rectification, erasure or closure of personal data that is being processed in violation of this law, particularly due to the incomplete or incorrect nature of such data, or because its processing is prohibited by law. The data controller is required to carry out the necessary rectifications free of charge, for the benefit of the applicant, within ten (10) days of being notified.

The last paragraph of Article 35 of this law has confirmed that this right (the right to rectification) is not personal and can be used by the heirs of the data subject, after their death.

Fourth, the right to object:

The right to object is one of the fundamental rights granted by Law No. 18-07 to the data subject in order to protect their privacy.

The first paragraph of Article 36 of the same law states that: "The data subject has the right to object, for legitimate reasons, to the processing of his or her personal data..."

It is logical that this right should be exercised by a request from the data subject to the data controller. The data subject must specify the legitimate reasons on which they rely in objecting to the processing of their personal data. The legislator has provided some grounds for objection, such as the use of data relating to the data subject for advertising purposes, particularly commercial ones, by the current data controller or a subsequent data controller. (Al-Ayari, 2005, p. 25)

Article 36, paragraph three, excludes two cases in which the data subject can not exercise their right to object if:

- **The processing is in response to a legal obligation,** as is the case for the processing carried out by customs or tax authorities.

- **If the data subject has expressly waived the exercise of this right in the document that authorizes the processing**. Therefore, it is necessary for the data controller to inform the data subject whether they should exercise the right to object or not

- **Fifth, the prohibition of direct marketing :**

According to Article 3/20 of Law No. 18-07, direct marketing is defined as: "The sending of any message, regardless of its medium or nature, intended for the direct or indirect promotion of goods or services or the reputation of a person who sells goods or provides services," whether this direct marketing is carried out by a communication mechanism, a remote reproduction device, email, or any other means using technologies of a similar nature, using the data of a natural person in any form, without their prior consent. This concerns advertising and commercial messages that are sent to the data subject.

However, the legislator authorized and licensed the process of direct marketing via email if the data was requested directly from the recipient, in the context of the sale or provision of services.

1.2 Obligations of the person responsible for processing personal data

The legislator has imposed on the data controller the need to take a number of measures to ensure the safety and confidentiality of the processing of personal data. The data controller is also required to process personal data related to electronic authentication and signature services. In addition, the data controller is required to process this data in the field of electronic communications. Finally, the data controller must follow certain procedures to transfer data to a foreign country. The following is a detailed description of these obligations.

First, the obligation to ensure the safety and confidentiality of the processing of personal data:

Based on Article 38 of Law No. 18-07 mentioned above, the person responsible for processing, and if necessary the subprocessor, is obligated to put in place appropriate technical and organizational measures to protect data of a personal nature from risks that may befall it, such as accidental or unlawful destruction, accidental loss, damage, publication or access. Unlicensed persons, especially when the processing requires sending data over a specific network and protecting it from any form of unlawful processing.

As for technical measures, a group of technologies can be used, such as encryption, encryption, personal access, or anti-viruses. As for organizational measures, they relate to protecting access to some places, for example, monitoring employees, or maintaining equipment such as computer programs, etc.

As for ensuring the confidentiality of processing, pursuant to Article 40 of Law-18-07, the person responsible for processing and persons who have access to data of a personal nature during the exercise of their duties are required to maintain professional confidentiality even after the end of their duties. In the event of a violation, they are subject to the penalties stipulated in the Penal Code related to disclosing professional secrets.

In order to ensure the confidentiality of personal data, no person working under the authority of the person responsible for the processing or the authority of a subprocessor who accesses data of a personal nature may process this data without the instructions of the person responsible for the processing, except in the case of carrying out a legal obligation

Second, the obligation to process personal data related to electronic authentication and signature services :

This obligation falls to electronic authentication service providers who issue qualified electronic certificates. For this purpose, the electronic authentication service provider collects personal data. In this case, the provider must comply with the purpose of processing and may not process the data for purposes other than those for which it was collected.

Third, the need to take certain measures in the event of processing personal data in the field of electronic communications :

According to Article 43 of the Algerian Law on the Protection of Personal Data, if the processing of personal data in public electronic communications networks leads

to its destruction, loss, disclosure, or unauthorized access, the service provider must immediately inform the National Authority and the data subject if this leads to an infringement of their privacy, unless the National Authority decides that the necessary safeguards to protect the data have been taken by the service provider (Article (43) Law No18-07, 2018).

The service provider is also required to keep a detailed record of violations related to personal data and the measures taken in relation to them.

Fourth - The obligation of the person responsible for processing to obtain a license from the national authority in the event of transferring data of a personal nature to a foreign country:

This is on the condition that the country to which the data is transferred provides adequate protection for the private life, freedoms and fundamental rights of individuals regarding the processing to which this data is or may be subjected, while sending and transferring data of a personal nature to a foreign country is prohibited when this may lead to a violation of public security. Or the vital interests of the state.

Conclusion:

Most countries in the world celebrate the tenth anniversary of World Data Protection Day, which falls on January 28 of each year ,which falls on January 28 each year. The purpose of this celebration is to raise awareness of a fundamental human right, namely the sanctity of personal data in the context of electronic processing. This is to sensitize people to the risks that threaten it, which have led to the enactment of legislation against activities of attacks on informational privacy in various global systems. This is what led the Algerian legislator to enact Law No. 18-07 on the Protection of Natural Persons in the Field of Processing of Personal Data, which achieves a kind of stability and trust in favor of the electronic consumer, and is an encouraging factor for individuals to deal with electronic transactions, such as e-commerce.

In order to enhance the legal system in the field of personal data protection and updating it, the following recommendations can be proposed:

- Entities that deal with personal data must take all necessary precautions to ensure the security of this data through high-tech procedures that ensure an appropriate level of protection for it.
- Urgent issuance of regulatory and implementing laws complementary to Law No. 18-07 on the Protection of Personal Data for the immediate activation and operation of its provisions as soon as possible (such as procedures for exercising the right of access and specifying the conditions and methods of keeping the national register, etc.).
- Reconciling security requirements with the protection of personal data, provided that processing in this case is done to the narrowest extent possible to protect the fundamental rights and freedoms of individuals.
- The need for individuals to be aware of their personal data and to be alerted to the risks that surround it, and the damage that may befall them from excessive exposure to it, through the media and others.

- Approval of codes of conduct in the field of personal data protection, followed by employees of entities responsible for processing personal data.

Sources and reference :

Al-Ayari, K. (2005, July). Legal protection of personal data. (E. (Center for Legal and Judicial Studies/Ministry of Justice and Human Rights, Éd.) *Journal of Judiciary and Legislation,, Issue 7*(Year 47).

Al-Maqata, M. A. (1992). *Protecting the private life of individuals and its guarantees in the face of computers, a comparative critical analytical study of the right to privacy, applications in Kuwaiti law.* Kuwait:: Kuwait University Press.

Article (43) Law No18-07, (2018, June 10). relating to the protection of natural persons in the field of processing of personal data. *J.J.R., 34*. algeria, algeria.

Baqi, J. A. (2001). *Criminal Law and the Internet,.* cairo: Dar Al-Fikr Al-Arabi.

Ben Qara, A. M. (2016, Jun). The right to information privacy between technology challenges and the reality of protection. *Journal of Legal and Political Research, issued by the Faculty of Law and Political Science,* (sixth issue).

Eoghan Casey. (2004). *Digital Evidence and Computer Crime—Forensic Science, Computers and the Internet.* London: Second Edition , Academic Press.

Fikry., A. A. (2007). *Information systems crimes, a comparative study.* cairo: New University House.

Freeland, C. (2007, May 7 – 8.). *Basel Committee Guidance on Corporate Governance for Banks, paperpresented to: Coorporate Governance and Reform: Paving the Way to Financial Stability and Development,* Cairo.

Jabri., S. A. (2005, December 18-20) . Information security and individual privacy. *International Conference on Electronic Information Security, Together towards a secure digital transaction,*. Muscat, Sultanate of Oman.

Law. (16-01; 2016, March 6). . Constitutional amendment. To the Algerian Official Gazette. *Algerian Official Gazette(14)*. Algeria.

Muhammad, K. A. (2020). Artificial intelligence and the law - a critical comparative study in French and Qatari civil legislation - in light of the European rules in the Civil Code for Robotics of 2019 and the European Industrial Policy for Artific. *Journal of Legal Studies*. doi: https://doi.org/10.54729/2958-4884.1059

Principles of United Nations System Organizations on Personal Data Protection and Privacy, U. (UNESCO. 2018, October 11, 11). *UNESCO, and was officially adopted by the High-level Administrative Committee at its thirty-sixth meeting.* Récupéré sur https://www.unsystem.org/privacy-principles

Tanuary, ". (1974, febrary). Law and computer technology. *vol.7* .(n ° 1.).

Zarrouk., A. H. (2013). *Legal regulation of the digital Morocco.* Morocco: Distributed by Al-Rashad Library - Settat.