LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. 10(2025)

PROTECTING PERSONAL DATA IN THE AGE OF ARTIFICIAL INTELLIGENCE: CHALLENGES AND SOLUTIONS

Benamrane Souhaila[1], Atoui ouided[2], Benachi Amel[3], Djebaili Sabrina[4]

[1]Abbes Laghrour University Of Khenchela ,State Laboratory for Health and Nutrition, Social Security
[2]University center Mersli Abdellah-tipaza**,** Laboratory of constitutional institutions and political systems
[3]Abbes Laghrour University Of Khenchela, Laboratory of legal, political andsharia, Social Security research
4Abbes Laghrour University Of Khenchela, Laboratory of legal, political andsharia, Social Security research

souhila.benamrane@univ-khenchela.dz[1]
atoui.ouided@cu-tipaza.dz[2]
benachi.amel@univ-khenchela.dz[3]
sabrina.djebaili@univ-khenchela.dz[4]

***Author correspondant :Benamrane Souhaila**

Received: 10/03/2025 Accepted:01/06/2025 Published: 15/07/2025

Abstract:
The world is currently experiencing advanced technological conditions, where artificial intelligence (AI) is increasingly used in various aspects of life. One of the critical issues raised by this new technology is the protection of individuals' personal data. Despite the benefits of AI, it can pose a threat to the privacy and personal security of individuals. Thus, in anticipation of enforcing Law No. 18-07 concerning the protection of natural persons in the processing of personal data, starting from August 2023, this research paper aims to highlight the most important legal measures adopted by legislators to protect personal data. There must be a balance between benefiting from AI and protecting personal data, which can only be achieved through legal intervention. The findings from studying this topic suggest that protecting personal data amidst increased AI usage requires comprehensive cooperation between the public and private sectors, in addition to providing necessary legislation and enhancing public awareness.

Keywords: Personal Data; Protection; Artificial Intelligence; Data; Personal Nature.

Introduction:

Artificial intelligence (AI) aligns with technologies capable of processing hybrid sources, particularly unstructured data. It has experienced a real surge in recent years. Perhaps for the first time, intangible activity becomes independent of humans. It is no longer about executing a program at the will and under the control of a human; rather, it involves nurturing a form of thought that, although conceived by humans, tends to some extent to liberate itself from them. Consequently, increasingly complex tasks are delegated to autonomous technological processes. However, this autonomy could potentially infringe on personal liberties. Among these liberties, identified by foundational texts and supreme courts, are the freedom of movement and freedom of opinion, which rely on the autonomy of will, and the right to privacy. The latter is closely linked to the home, correspondence, and intimate relationships that must remain confidential.

The disruption in our lives due to the expansion of artificial intelligence has been of particular interest to public authorities since the emergence of applications that have drawn the attention and concern of citizens. Indeed, these practices have distorted individual desires and raised questions about a fundamental principle of our legal system: ensuring individual liberties. Are we not opening the doors wide to excessive trust in machines, leading individuals to relinquish their judgment capabilities? This implies adapting current regulations by establishing a new generation of guarantees and fundamental rights specific to digital technology. Consequently, public authorities are obligated to adopt legal rules that allow the development of individual liberties in the face of risks posed by artificial intelligence. The law must evolve towards an appropriate legal framework that enables humans to maintain their capacity for judgment and autonomy. However, regulating

algorithms remains challenging due to the scalability of technology and the secretive, competitive nature of developments.

Study problem:

The problem of this study can be formulated in the following main question:

Given the increasing use of artificial intelligence, what are the mechanisms for protecting personal data?

To address this issue, it is essential to explore two main axes:

- Conceptual Introduction to Artificial Intelligence and Personal Data
- The Legal Framework for Protecting Personal Data in the Face of Artificial Intelligence and Its Limits

Section I: Conceptual Introduction to Artificial Intelligence and Personal Data

A) The Concept of Artificial Intelligence:

The concept of artificial intelligence emerged in the 1950s, authored by mathematician Alan Turing in his book "Computing Machinery and Intelligence". In this work, Turing proposes the possibility of equipping machines with a form of intelligence. He also introduced a test now known as the "Turing Test", which aims to assess the intelligence of computer systems. In this test, a person interacts blindly with another human and then with a machine programmed to formulate logical responses. If the person cannot distinguish between the human and the machine, it means that the machine has passed the test. According to Turing, if a machine succeeds in this test, it can be considered intelligent(1).

1- Definition of Artificial Intelligence:

Researchers and philosophers have varied in defining the concept of artificial intelligence, and below, some basic and contemporary concepts are presented.

Artificial intelligence is defined as: "The scientific and technical current that includes methods, theories, and technologies aimed at creating machines capable of simulating intelligence(2)." This concept highlights the scientific nature and does not rely solely on the technical feature to form artificial intelligence, with the goal of reaching human intelligence capabilities.

It is also defined as: "An autonomous, non-biological learning system(3)." Additionally, it is defined as: "A computer system that has the capability to mimic human behavior, intelligence, performance, and tasks(4)."

From this concept, we infer that it is a system directed towards learning, characterized by autonomy, and that it is purely mechanical, with no human or animal mind intervention.

Through the concepts mentioned above, we can derive a definition of artificial intelligence as an attempt to use machines and modern technological techniques as a means to perform mental work (intelligence, reasoning, logic, learning, and self-organization) that the human mind performs, characterized by several features including(5); being non-biological (organic) and autonomous, automating intelligent systems, being perceptive and responsive, capable of self-learning, decision-making to action, and algorithms for learning and self-organization.

2- The Importance of Artificial Intelligence:

Given the multitude of uses for artificial intelligence, its importance is evident through(6):

- Achieving inclusion and equity, as the 2030 Agenda for Sustainable Development acknowledges that digital technologies hold great potential to accelerate progress, bridge the digital divide, support the growth of inclusive knowledge societies for all based on human rights, achieve gender equality, and build capacity. Thus, they are crucial in achieving the seventeen Sustainable Development Goals.
- Contributing to education with a priority for low-resource communities and vulnerable groups.
- Providing learning opportunities for students and other learners, including disadvantaged groups based on gender, disability, socio-economic status, cultural background, minority languages, or geographical location.

3- Fields of Artificial Intelligence:

Artificial intelligence applications span all aspects of human life and are divided into[7]:

Explored Fields: which include:

- Professional Services: Executives, politicians, lobbying bodies, judges, and lawyers.
- Enhancing Decision-Making Processes.
- Exploration in Environmental Protection and Space Exploration.
- Personal Services Using Robots, especially in areas of finance, security, mobility, entertainment, education, health, and food.
- Urban Planning: Smart cities, designed cities.

Fields in Need of Exploration: Housing, conflict resolution, personal relationships, ethics, religion, meaning, media, population control, employment, governance.

B) The Concept of Personal Data:

The right to privacy and the protection of personal data and private lives of individuals have garnered the attention of the majority of legislations, bodies, and international organizations, with the Universal Declaration of Human Rights of 1948 at the forefront. Article 12 of the Declaration states[8]: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." Similarly, the International Covenant on Civil and Political Rights, ratified by the UN General Assembly on December 16, 1966, states in Article 17: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation," and that: "Everyone has the right to the protection of the law against such interference or attacks[9]."

Following this directive, Algeria has prioritized the protection of personal data, making it a constitutional principle. Article 47 of the constitutional amendment states: "Every person has the right to the protection of his private life and honour. Every person has the right to the confidentiality of his correspondence and private communications in any form. The rights mentioned in the first and second paragraphs may not be infringed except by a justified order from the judicial authority. The protection of individuals in the processing of personal data is a fundamental right. The law penalizes any violation of these rights[10]."

1- Definition of Personal Data:

Article 03 of Law No. 18/07 defines personal data as: "Any information, regardless of its medium, related to an identified or identifiable person, referred to hereafter as 'the data subject,' directly or indirectly, especially by reference to an identification number or one or more factors specific to their physical, physiological, biometric, psychological, economic, cultural, or social identity[11]."

According to the second paragraph of the same article, the data subject is: "Any natural person whose personal data is being processed[12]."

Some legal scholars have also attempted to define personal data as: "Any information that directly identifies a person or through its processing or analysis, whether it is stored on paper, electronically, or otherwise, except for information related to public life[13]."

The scope of personal data has expanded with the development of the internet. It no longer just includes the name, surname, and postal address, but has grown to encompass a person's image, voice, and a range of other data related to their financial capabilities, behaviors, habits, preferences, tastes, and, most significantly, biometric data related to the human body[14].

Since the right to personal data is closely linked to the right to privacy and is an integral part of the right to a private life—which the constitutional founder has guaranteed protection for—it is necessary to delve into the definitions that have been articulated regarding it: The right to privacy is defined as: "The individual's right to live their life away from the following actions: interference in family or home life, intervention in their physical and mental being or moral or mental freedom, attacks on their honor or reputation, exposure under false light, broadcasting events related to their private life, use of their name or image, spying and peeping, observation and interference in

correspondence, misuse of private written or oral communication means, and disclosure of information obtained by virtue of trust and profession[15]."

2- Processing of Personal Data:

The Algerian legislator defined the processing of personal data through Law No. 18/07 as: "Any operation or set of operations carried out with or without the aid of automated means on personal data, such as collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction[16]."

2-1 Rights of the Data Subject:

The Algerian legislator, through the provisions of Law No. 18/07 concerning the protection of personal data, outlined the rights of the data subject regarding the processing of their personal data:

2-1-1 Right to Information:

Article 32 of the law obliges the data controller, or their representative, to explicitly and unambiguously inform each data subject whose personal data is processed about the following information: the identity of the data controller, the purposes of the processing, and any other useful information unless it has been previously provided.

Exceptions to the mandatory information apply if it is impossible to inform the data subject, in which case the national authority must be notified with the reason for the impossibility. The obligation to inform is also waived if the purpose of processing is journalistic, artistic, or literary[17].

2-1-2 Right to Access:

Article 34 of Law No. 18/07 enshrines the right of the data subject to access their personal data and is considered a human right.

Under this right, the data subject has access to their personal data undergoing processing, the purposes of processing, categories of data involved, recipients, and any available information about the source of the data[18].

2-1-3 Right to Rectification:

The right to rectification refers to the right of any person to obtain from the data controller, free of charge, the updating, rectification, erasure, or blocking of personal data that is processed unlawfully, incomplete, or inaccurate within a maximum period of 10 days from notification.

In case of refusal, the data subject has the right to submit their request to the independent authority, which will take appropriate action. It is necessary to inform others who received the personal data of any rectification, update, erasure, or blocking of personal data. The right to rectification passes to the heirs in the event of the data subject's death[19].

2-1-4 Right to Object and Prevent Direct Marketing:

The data subject has the right to object to the processing of their personal data for advertising or commercial purposes by the data controller[20]. According to Law No. 18/07, they may prevent direct marketing through any electronic means unless they have given their prior consent[21].

2-2 Obligations of the Data Controller:

The Algerian legislator has outlined the obligations of the data controller through the provisions of Law No. 18/07, which primarily revolve around:

2-2-1 Confidentiality and Integrity of Processing:

The data controller is obligated to take all technical measures to protect and secure personal data against hacking, damage, and any unlawful use. The precautionary measures are reinforced as the personal data becomes more valuable and important. The data controller is also obligated to provide adequate guarantees related to safety procedures. Moreover, the data controller and persons who have accessed the data must maintain professional secrecy even after their duties have ended[22].

2-2-2 Processing of Personal Data in the Field of Electronic Certification and Electronic Communications[23]:

The law mandates that electronic certification service providers process personal data solely for the issuance and preservation of certificates associated with electronic signatures, unless expressly consented to for other purposes. Providers of electronic communication services, after taking all

necessary safeguards to protect the data, must notify the national authority and the data subject if there is any infringement of privacy in cases of damage, loss, disclosure, or unauthorized access[24].

2-2-3 Transfer of Data to Foreign Countries:

A data controller may not transfer personal data to a foreign country without authorization from the independent authority, ensuring that the foreign country protects privacy, freedoms, and rights of individuals during processing, particularly by verifying appropriate security measures within the foreign country. Such data must not affect public security or vital interests of the state. The data controller is exempt from these conditions in cases specified in Article 45 of the same law, including: explicit consent from the data subject, or if the transfer is necessary to preserve the life of the data subject or for the public interest, among other situations exclusively listed in the article[25].

Section II: The Legal Framework for Protecting Personal Data in the Face of Artificial Intelligence and its Limits

The Algerian Constitution ensures the protection of personal freedoms, emphasizing that the law will punish any violation of individuals' private life, their honor, and any breach of the confidentiality of correspondence and private communications in any form.

Furthermore, Law No. 18-07, concerning the protection of natural persons in the processing of personal data, has indeed imposed a number of principles that require reinforcement (First Requirement). It also highlights the role of the independent authority responsible for the protection of personal data (Second Requirement).

A) Principles that Require Strengthening by the Algerian Legislator in Facing Artificial Intelligence:

There are numerous challenges in protecting personal data in the context of artificial intelligence. One such challenge is ensuring the security of the systems used for collecting and storing data. It is essential that robust and reliable intelligent systems are designed and implemented to protect data from any leaks or attacks. In this regard, the Algerian legislator has provided for the protection of personal data under Article One, explicitly stating that the purpose of this law is to establish rules for protecting natural persons in the processing of their personal data. The legislator has excelled in this respect, although there are remarks concerning the lack of treatment of data related to legal entities. In this context, we will discuss the provisions for protecting privacy and then the fundamental principles for the protection of personal data (Second Subsection).

Challenges include not only the technical aspects of securing data but also addressing the broader implications of AI, such as bias, discrimination, and the potential for invasive surveillance that can infringe upon fundamental human rights and freedoms. The response by the legislature needs to evolve continuously to address these emerging issues effectively. This involves not only creating secure infrastructures but also ensuring that AI technologies respect privacy norms and are transparent and accountable in their operations.

1- Provisions for Protecting Privacy:

The right to privacy is one of the most important human rights and belongs to the first generation of rights articulated in the Universal Declaration of Human Rights of 1948. Article 12 of the Declaration states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks[26]." Similarly, the International Covenant on Civil and Political Rights of 1966, through its Article 17, stipulates: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks[27]."

Both the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights emphasize legal protection for privacy. The United Nations Human Rights Committee, commenting on Article 17 of the Covenant, noted that the right to privacy includes protection against all such interferences and assaults, whether they come from state authorities or from natural or legal persons. However, the expansion in defining the reasons for assault opens up

opportunities for violations resulting from the use of artificial intelligence in breaching privacy, especially in monitoring individuals' movements and health status through the collection and processing of personal data, which are considered part of privacy.

In this context, General Comment No. 16 of the Human Rights Committee underscores the significance of personal data in privacy, granting individuals the right to verify the information held about them, the purposes of its storage, and the entity that holds it(28).

Infringing on privacy rights is considered a blatant violation of human rights and fundamental freedoms. As technology evolves and we face the challenges of artificial intelligence, it is crucial to maintain the right to privacy by ensuring the privacy and confidentiality of stakeholders and users.

The right to privacy is legally established in the Algerian Constitution and many other legal texts. Article 47 of the Algerian Constitution stipulates: "Every individual has the right to protect their private life and honor. Every individual has the right to the confidentiality of their correspondence and private communications in any form. These rights mentioned in the first and second paragraphs cannot be infringed upon except by a justified order from the judicial authority. Protecting individuals in the processing of personal data is a fundamental right. The law penalizes any violation of these rights(29)."

Furthermore, Article 47 of the Algerian Civil Code states: "Anyone who suffers an unlawful attack on any of their inherent personal rights may demand the cessation of this attack and compensation for any damage incurred(30)."

Similarly, Article 93 of the Media Law states: "Violating the privacy of individuals and their honor and reputation is prohibited. The privacy of public figures cannot be violated directly or indirectly(31)."

With the increase in modern technologies, the risks to the right to private life have grown, and individuals are restricted in their interactions through the monitoring, storage, and processing of their personal data using information technology, such as surveillance or spying techniques. These actions represent a direct threat to private life and individual freedoms in their modern form, as part of a data bank, especially if exploited for purposes outside the control of the owner and without their knowledge.

The risks of artificial intelligence in violating the right to privacy include:

- **Violation of the confidentiality of personal data** through unlawful data processing, which gains a confidential nature, leading to potential data leaks due to non-compliance with legally stipulated conditions and methods(32).
- **Electronic spying**, defined in Article 3 of the Budapest Convention on Cybercrime of 2001 as: "The act of intercepting or capturing data transmitted remotely between two devices over the internet, or by translating electromagnetic emissions from a computer into data, using any technical means(33)."
- **Computer and email hacking**, defined as: "An unauthorized access to another's computer using sophisticated software under high technical and expert proficiency(34)."

Like other Arab countries, Algeria has adopted a law specifically for the protection of personal data, enacting Law No. 18-07 concerning the protection of natural persons in the processing of personal data. Article 02 of this law emphasizes that: "Personal data, regardless of its source or form, must be processed with respect for human dignity, private life, public freedoms, and must not infringe upon the rights, honor, and reputation of individuals(35)." This law has imposed specific rules and procedures for the processing of personal data.

2- Fundamental Principles for the Protection of Personal Data:

The Algerian legislator has integrated the fundamental principles for the protection of personal data into Chapter Two of the law, divided into two sections: the first concerning prior consent and data quality, and the second related to the procedural requirements before processing.

2-1 Prior Consent and Data Quality:

Law No. 18-07 emphasizes the necessity of explicit consent from the data subject for the processing of personal data, except where such consent has already been provided. If the data

subject is legally incapacitated, their consent is governed by the rules stipulated in the law. The data subject has the right to withdraw their consent at any time. Third parties may not access personal data being processed unless it is directly related to the duties of the data controller or the recipient, and only after prior consent from the data subject.

However, the consent of the data subject is not required if the processing is necessary:

- To comply with a legal obligation to which the data subject or the data controller is subject.
- To protect the life of the data subject.
- To execute a contract to which the data subject is a party, or to carry out pre-contractual measures taken at the data subject's request.
- To protect the vital interests of the data subject if they are physically or legally incapable of giving consent.
- To perform a task carried out in the public interest or in the exercise of official authority vested in the data controller or a third party who is privy to the data.
- To pursue a legitimate interest by the data controller or the recipient, considering the interests or fundamental rights and freedoms of the data subject[36].

In the case of processing personal data of a child, the consent of the child's legal representative is required, or authorization from the competent judge if the child's interest so requires[37].

Conditions for Processing Personal Data includes:

- Data must be processed lawfully, fairly, and transparently.
- Collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
- Adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data that is inaccurate, with respect to the purposes for which they are processed, is erased or rectified without delay.
- Kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed[38].

2-2 Pre-processing Procedures:

Article 12 of Law No. 18-07 mandates that every personal data processing operation must be subject to prior declaration to or authorization from the National Authority.

2-2-1 Declaration:

The declaration involves a commitment to conduct the processing at the National Authority or via electronic submission[39]. It must include the following:

- The name and address of the data controller and, if applicable, the name and address of their representative.
- The nature of the processing, its characteristics, and the intended purpose.
- A description of the category or categories of the concerned individuals and the data or categories of personal data related to them.
- The recipients or categories of recipients who may receive the data.
- The nature of the data intended to be transferred to foreign countries.
- The duration of data retention.
- The interest in which the concerned individual may, if necessary, exercise the rights granted under the provisions of Law 18-07, as well as measures taken to facilitate the exercise of these rights.
- A general description that allows for an initial assessment of the adequacy of the measures taken to ensure the confidentiality of the processing.
- The interconnection 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 of charge or for a fee.

In the event of any change or deletion affecting the data, the National Authority must be notified[40].

2-2-2 Authorization:

Article 17 of Law 18-07 stipulates: "The National Authority decides to subject the processing concerned to a prior authorization regime when, upon reviewing the declaration submitted to it, it determines that the intended processing involves apparent risks to the respect and protection of private life and the fundamental freedoms and rights of individuals."

The decision of the National Authority must be justified and communicated to the data controller within ten days following the date of the declaration.

The legislator has prohibited the processing of sensitive data except those related to the public interest and with explicit consent from the concerned individual, in addition to other cases stipulated by law[41].

B) The National Authority for the Protection of Personal Data

The Algerian legislator has established a National Authority for the Protection of Personal Data, endowed with specific competencies in addition to a set of penal provisions which will be discussed through two branches: the theoretical framework of the National Authority (First Branch), and the administrative and penal protection of personal data (Second Branch).

1- Theoretical Framework of the National Authority

In this section, we will explore the concept of the National Authority for the Protection of Personal Data (first), followed by the formation of the National Authority (second).

1-1 Concept of the National Authority for the Protection of Personal Data

Generally, independent administrative authorities, and particularly the National Authority, are not tasked with administrative duties but rather regulatory functions, taking on the role of maintaining certain balances within society. The National Authority is tasked with preserving personal data. The concept of this National Authority can be defined as: "Administrative bodies that are non-judicial and have decision-making power. They are not required to have an independent legal personality, and they are not subject to any presidential or supervisory control. The law has entrusted them with the task of regulating sensitive sectors in the state[42]." It is worth noting that the legal nature of independent administrative authorities has not been fully established by legal text. However, for the National Authority for the Protection of Personal Data, its legal nature is explicitly defined in Article 22 of Law No. 18/07, which states:

"An independent administrative authority for the protection of personal data is established under the President of the Republic, hereinafter referred to as 'the National Authority.' Its headquarters are located in Algiers. The National Authority has legal personality and financial and administrative independence. Its budget is recorded in the state budget and is subject to financial control according to applicable legislation. The National Authority prepares its internal regulations, which define, in particular, the methods of its organization and operation, and approves them."

The Authority is responsible for protecting any information, regardless of its medium, related to an identified or identifiable person, directly or indirectly, especially by referring to an identification number or one or more factors specific to their physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity[43].

In the context of implementing the provisions of the Constitution regarding the protection of individual rights and freedoms as stated in Article 47 of the Algerian Constitution, the legislator has designated a specific legal text for the protection of personal data, Law No. 18-07. Article 2 of this law emphasizes that: "Personal data, regardless of its source or form, must be processed with respect for human dignity, private life, and public freedoms and must not infringe upon the rights, honor, and reputation of individuals."

1-2 Composition of the National Authority

According to Article 23 of Law No. 18-07, the National Authority for the Protection of Personal Data is composed of the following members:

- Three (3) personalities, including the president, selected by the President of the Republic from among those with expertise in the field of the Authority's work.

- Three judges, proposed by the Supreme Council of the Judiciary from among the judges of the Supreme Court and the Council of State.
- A member from each chamber of Parliament, chosen by the president of each chamber after consulting with the leaders of the parliamentary groups.
- A representative from the National Human Rights Council.
- A representative from the Ministry of National Defense.
- A representative from the Ministry of Foreign Affairs.
- A representative from the Ministry of the Interior.
- A representative from the Ministry of Justice, Keeper of the Seals.
- A representative from the Ministry responsible for Post, Telecommunications, Technology, and Digitalization.
- A representative from the Ministry of Health.
- A representative from the Ministry of Labor, Employment, and Social Security.

Members of the National Authority are selected based on their legal and/or technical expertise in the field of personal data. The Authority may also call upon any qualified individual who can assist in its operations. The president and members of the National Authority are appointed by presidential decree for a term of five years, which is renewable.

The composition of the National Authority reflects a diversity of expertise and affiliations from different sectors. This diversity is logical since the National Authority is tasked with judicial-like responsibilities, necessitating the inclusion of judges in its formation. This structure ensures a comprehensive approach to personal data protection, incorporating diverse perspectives from various sectors involved in data handling and privacy issues[44].

2- Competencies of the National Authority for the Protection of Personal Data:

2-1 Administrative Protection:

As per Article 25 of Law No. 18-07, the general competencies of the National Authority involve overseeing the compliance of personal data processing with the provisions of Law 18-07, ensuring that the use of information and communication technologies does not pose any risks to individuals' rights, public freedoms, and private life. The tasks in this regard include:

- Granting Licenses and Receiving Declarations: Handling applications related to the processing of personal data.
- Informing Individuals and Data Controllers: Educating about their rights and obligations under the law.
- Providing Consultations: Advising individuals and entities that engage in data processing or conduct experiments or experiences that may lead to such processing.
- Receiving Grievances and Complaints: Dealing with issues related to the implementation of personal data processing and informing the complainants of the outcome.
- Authorizing Data Transfer Abroad: Ensuring that data transfers outside the country comply with the conditions stipulated in the law.
- Ordering Necessary Changes: Mandating adjustments needed to protect processed personal data.
- Ordering the Closure, Withdrawal, or Destruction of Data: Enforcing the removal or destruction of data when necessary.
- Proposing Improvements to Legislative and Regulatory Frameworks: Suggesting enhancements to simplify and better the legislative and regulatory environment for personal data processing.
- Publishing Granted Licenses and Opinions: Disclosing licenses and advisory opinions in the national registry.
- Developing International Cooperation: Building cooperative relationships with foreign authorities having similar mandates, ensuring reciprocity in treatment.

- Issuing Administrative Sanctions: Enforcing penalties for non-compliance with data protection regulations.
- Establishing Standards for Data Protection: Setting benchmarks to guide data protection practices.
- Developing Codes of Conduct and Ethics: Outlining ethical guidelines and codes of conduct for data processing to ensure adherence to best practices.

Members of the National Authority are required, in the course of performing their duties, to maintain the confidentiality of the personal data they have access to in this capacity, even after they have completed their duties, unless there is a legal provision to the contrary(45).

The legislator has established a set of administrative procedures that the National Authority can resort to. The National Authority for the Protection of Personal Data can take a series of administrative actions against the data controller in case of a breach of the provisions set out in Law No. 18-07. These administrative actions are included in a special chapter from Article 46 to Article 48. These procedures can take the form of:

- A warning: A warning is not considered a penalty by the National Authority but usually takes the form of an alert (warning) to remind the data controller of the obligation to correct the situation and take the necessary measures to make their activity compliant with the legal provisions stipulated in the Law No. 18-07 on personal data protection.
- A summons: It is a legal means granted by the legislator to the National Authority to notify and inform the data controller of their obligation to comply with the legal provisions of Law No. 18-07 within a specified period before resorting to the courts(46).
- Temporary withdrawal for a period not exceeding one year, or permanent withdrawal of the declaration or license: The National Authority can withdraw the declaration receipt or license immediately and without delay if it turns out after the processing subject to the declaration or license that it compromises national security, or is contrary to morals or public decency(47).
- A fine: Imposed against any data controller who unjustifiably refuses rights of information, access, correction, or objection. Or the responsible party who does not report to the National Authority as stipulated in Articles 14 and 16 of Law No. 18-07. The amount of this fine is 500,000 DZD.
- Regarding the notification required by Article 14 of Law 18-07, it relates to the information and data contained in the declaration and specified by the article; in case of any changes or deletions affecting the processing, the data controller must notify and inform the National Authority of these changes. If the notification is not made, a fine of 500,000 DZD is imposed.
- As for the notification stipulated in Article 16 of Law No. 18-07, it concerns declarations for processing operations intended to maintain a register open to public inspection or to any person who proves a legitimate interest in it. The obligation to declare does not apply in this case, but a data controller must be appointed who reveals their identity to the public and reports to the National Authority, and in case of non-notification, a fine of 500,000 DZD is imposed.

The law also stipulates that decisions made by the National Authority can be appealed before the State Council(48). This confirms the administrative nature of this authority, thus making its decisions subject to appeal before the State Council.

Additionally, the National Authority is granted procedural rules allowing it to conduct necessary investigations and inspect premises where data processing occurs, except for residential places. It is permitted, in the performance of its duties, to access processed data and all information and documents regardless of their medium.

The law emphasizes that professional secrecy does not apply in dealings with the National Authority. In this regard, in addition to judicial police officers and agents, other control agents

whom the National Authority may call upon to investigate and inspect crimes stipulated in Law 18-07 are involved, and their reports are directed to the public prosecutor.

The law ensures that a person whose rights, as legally guaranteed, have been violated, may request from the competent judicial authority to take precautionary measures to end this violation or to obtain compensation(49).

2-2 Penal Protection of Personal Data:

2-2-1 Penal Provisions:

Given the importance of personal data to the right to privacy of individuals, there is a necessity to establish punitive rules to protect it from threats. This was addressed by the Algerian legislator through the enactment of Law No. 18-07 on the protection of personal data processing, where Chapter Three from Articles 54 to 74 lays out penal provisions criminalizing violations concerning personal data during processing. A range of penalties has been established for entities that do not comply with the provisions of this law.

Any breach of the rules of Law No. 18-07 is punishable with imprisonment from two to five years and a fine from 200,000 DZD to 5,000,000 DZD(50). Furthermore, anyone who processes personal data without the prior consent of the concerned individual is subject to imprisonment from one to three years and a monetary fine ranging from 100,000 DZD to 300,000 DZD. The same penalty applies to anyone who processes personal data despite the individual's objection, especially when targeted for commercial advertising or when the objection is based on legitimate reasons(51). Additional penalties are imposed for obstructing the work of the National Authority, including:

- Obstructing the conduct of on-site verification.
- Refusing to provide its members or agents, who are placed at its disposal, with necessary information and documents to carry out the task assigned to them by the National Authority, or by concealing or removing the mentioned documents or information.
- By providing information that does not match the contents of the records at the time of the request or failing to present it directly and clearly.

Violations are punishable with imprisonment from six months to two years and a financial penalty ranging from 60,000 DZD to 200,000 DZD(52).

Additionally, there are other penal provisions, as well as supplementary penalties that those who violate this law might face, as stipulated in the Penal Code. It is possible to order the deletion of all or part of the personal data that was processed and led to the commission of the crime. Members and employees of the National Authority are authorized to oversee the deletion of this data(53).

Conclusion:

In concluding this research paper, we have determined that the Algerian legislator, similar to comparative legislations, has established legal protection for personal data under Law No. 18/07 concerning the protection of personal data, which embodies the general principle enshrined by the constitutional founder, particularly through the provision of Article 47.

In this context, the law carries a set of principles and mechanisms that enhance the protection of personal data from any violation, breach, piracy, or infringement of privacy. Foremost among these mechanisms is the National Authority for the Protection of Personal Data, despite some reservations regarding its failure to address data related to legal entities, in addition to the lack of activation of the independent National Authority and the absence of elected members in its composition, which affects its transparency.

Protecting personal data in the context of increasing use of artificial intelligence requires comprehensive cooperation between the public and private sectors, in addition to providing necessary legislation and enhancing public awareness.

Citations:

1- Futura, "Artificial Intelligence: What is it?",Futura-Sciences, consulted on 08/12/2024.

2- Samia Chehi Qammoura et al., "Artificial Intelligence Between Reality and Expectation: A Technical and Field Study," presented at the International Conference on Artificial Intelligence: A New Challenge for Law, November 26-27, 2018, Algiers, p. 5.
3- Osinde A. Osoba, William Welser IV, "The Risks of Artificial Intelligence to Security and the Future of Work," RAND Corporation, www.rand.org,consulted on05/11/2024.
4- Leila Ben Barghouth, "Cybersecurity and Protection of Digital Data Privacy in Algeria in the Age of Digital Transformation and Artificial Intelligence: Threats, Technologies, Challenges, and Countermeasures," International Journal of Social Communication, Abdelhamid Ibn Badis University - Mostaganem, Volume 10/Issue 01 for the year 2023, p. 448.
5- Osinde A. Osoba, William Welser IV, op. cit., p. 7.
6- UNESCO, "Artificial Intelligence and Inclusion: A Concept Note," Mobile Learning Week, (Education 2030) Paris, March 2-6, 2020, p. 4.
7- Osinde A. Osoba, William Welser IV, op. cit., p. 4.
8- The Universal Declaration of Human Rights, United Nations,UN Universal Declaration of Human Rights, consulted on 24/11/2024.
9- The International Covenant on Civil and Political Rights, December 16, 1966, University of Minnesota Human Rights Library, consulted on 25/11/2024.
10- The Official Gazette of the Algerian Republic, Issue No. 82, published on: 15 Jumada Al-Awwal 1442 AH corresponding to December 30, 2020, p. 04.
11- Law No. 18-07 dated: 25 Ramadan 1439 AH corresponding to June 10, 2018, concerning the protection of natural persons in the processing of personal data, Official Gazette, Issue No. 34 for the year 2018.
12- Article 03/02 of Law No. 18-07 concerning the protection of natural persons in the processing of personal data.
13- Mohamed El Aidani, Youssef Zarrouk, "Protection of Personal Data in Algeria in Light of Law No. 18/07," Maalim Journal for Legal and Political Studies, Issue 05, December 2018, p. 119.
14- Aicha Ben Qara Mustafa, "Mechanisms for the Protection of Personal Data in Algerian Legislation According to the Provisions of Law No. 18/07," Journal of Legal and Political Sciences, Volume 10, Issue 01, April 2019, p. 747.
15- Salim Jalad, "The Right to Privacy between Guarantees and Controls," Master's thesis in Sharia and Law, Human Rights specialization, Department of Islamic Sciences, Faculty of Humanities and Islamic Civilization, University of Oran, Algeria, 2012-2013, p. 15.
16- Article 03/03 of Law No. 18-07 concerning the protection of natural persons in the processing of personal data.
17- Article 33 of Law No. 18-07 concerning the protection of natural persons in the processing of personal data.
18- Fatiha Hezam, "Legal Guarantees for Processing Personal Data," Ijtihad Journal for Legal and Economic Studies, Volume 08, Issue 4, 2019, p. 286.
19- Article 35 of Law No. 18-07 concerning the protection of natural persons in the processing of personal data.
20- Article 36 of Law No. 18-07 concerning the protection of natural persons in the processing of personal data.
21- Article 37 of Law No. 18-07 concerning the protection of natural persons in the processing of personal data.
22- Articles 38-40 of Law No. 18-07 concerning the protection of natural persons in the processing of personal data.
23- Articles 42-43 of Law No. 18-07 concerning the protection of natural persons in the processing of personal data.
24- Mohamed El Aidani, Youssef Zarrouk, op. cit., p. 126.
25- Articles 44-45 of Law No. 18-07 concerning the protection of natural persons in the processing of personal data.
26- The Universal Declaration of Human Rights, adopted in 1948.
27- The International Covenant on Civil and Political Rights, adopted by the UN General Assembly on December 16, 1966, under Resolution 2200A (XXI), which did not enter into force until March 23, 1976.
28- Mohamed El Hadi El Souhaili, "Artificial Intelligence Developments and the Requirements for Protecting Rights and Fundamental Freedoms," Islamic World Organization for Education, Science, and Culture, Legal Affairs Administration at ISESCO, p. 23.
29- The 1996 Constitution amended by Law No. 02/03 dated April 10, 2002, Official Gazette, Issue No. 25, and Law No. 08/19 dated November 15, 2008, and Law No. 16/01 dated March 6, 2016, Official Gazette, Issue No. 14, and the Presidential Decree No. 20/442 dated December 30, 2020, concerning the issuance of the constitutional amendment ratified in the referendum on November 1, 2020, Official Gazette, Issue No. 82.
30- Order No. 75-58 dated September 26, 1975, corresponding to 20 Ramadan 1395, which includes the amended and supplemented Civil Code, Official Gazette, Issue No. 78.
31- Organic Law No. 12-05 dated January 12, 2012, corresponding to 18 Safar 1433, related to Media, Official Gazette, Issue No. 2.
32- Khadija Dahbi: "The Right to Privacy in the Face of Cyber Attacks (Comparative Study)," The Professor Researcher Journal for Legal and Political Studies, Issue 8, December 2007, p. 130.
33- Article 3 of the Budapest Convention on Cybercrime, 2001.
34- Khadija Dahbi, op. cit., p. 151.
35- Law No. 18-07 dated June 10, 2018, corresponding to 25 Ramadan 1439, concerning the protection of natural persons in the processing of personal data, Official Gazette, Issue No. 34 of 2018.

36- Article 7 of Law No. 18-07, Op. Cit.
37- See Article 8 of Law No. 18-07, Op. Cit.
38- See Article 9 of Law No. 18-07, Op. Cit.
39- See Article 13 of Law No. 18-07, Op. Cit.
40- Article 14 of Law No. 18-07, Op. Cit.
41- See Article 15 of Law No. 18-07, Op. Cit.
42- Souhila Ben Imran, "The Legal System of Independent Administrative Authorities in Algerian Legislation," doctoral thesis, Administrative Law, Faculty of Law and Political Science, University of Badji Mokhtar Annaba, 2019, p. 28.
43- See Article 3 of Law No. 18-07 dated June 10, 2018, concerning the protection of natural persons in the processing of personal data, Official Gazette, No. 34 of 2018.
44- Marie-José Guedon, "Les autorités administratives indépendantes," LGDJ, Paris, 1991, p. 70.
45- See Articles 25 and 26 of Law No. 18-07, Op. Cit.
46- Aicha Ben Qara Mustafa, "Mechanisms for the Protection of Personal Data in Algerian Legislation According to the Provisions of Law No. 18-07," Journal of Legal and Political Sciences, Hamma Lakhdar University, El Oued, Volume 10, Issue 01, pp. 746-761, April 2019.
47- See Article 48 of Law No. 18-07, Op. Cit.
48- See Article 46 of Law No. 18-07, Op. Cit.
49- See Article 49 of Law No. 18-07, Op. Cit.
50- See Article 54 of Law No. 18-07, Op. Cit.
51- See Article 07 of Law No. 18-07, Op. Cit.
52- See Article 61 of Law No. 18-07, Op. Cit.
53- See Article 71 of Law No. 18-07, Op. Cit.

Bibliography:

A- Legal Texts:

- The 1996 Constitution, amended by Law No. 02/03 dated April 10, 2002, Official Gazette No. 25; Law No. 08/19 dated November 15, 2008; Law No. 16/01 dated March 06, 2016, Official Gazette No. 14; and Presidential Decree No. 20/442 dated December 30, 2020, concerning the issuance of the constitutional amendment approved in the referendum of November 1, 2020, Official Gazette No. 82.
- Law No. 18-07 dated June 10, 2018, corresponding to Ramadan 25, 1439, concerning the protection of natural persons in the processing of personal data, Official Gazette No. 34 for the year 2018.
- Order No. 75-58 dated Ramadan 20, 1395, corresponding to September 26, 1975, including the amended and supplemented Civil Law, Official Gazette No. 78.
- Organic Law No. 12-05 dated Safar 18, 1433, corresponding to January 12, 2012, related to media, Official Gazette No. 2.

B- Books

Marie-josé-GUEDON, "Les autorités administratives indépendantes", LGDJ, Paris, 1991, p. 70.

C- Theses:

- Souhaila Ben Imran, "The Legal System for Independent Administrative Authorities in Algerian Legislation," a doctoral dissertation in Administrative Law, Faculty of Law and Political Science, University of Badji Mokhtar, Annaba, 2019, p. 28.
- Salim Jalad, "The Right to Privacy Between Guarantees and Controls," a master's thesis in Sharia and Law, specialization in Human Rights, Department of Islamic Sciences, Faculty of Human Sciences and Islamic Civilization, University of Oran, Algeria, 2012-2013.

D- Newspaper articles:

- Aisha Ben Qara Mustafa, "Mechanisms for Protecting Personal Data in Algerian Legislation According to the Provisions of Law No. 18-07," Journal of Legal and Political Sciences, Hamma Lakhdar University, El Oued, Volume 10, Issue 01, Pages 746-761, April 2019.
- Khadija Dahabi, "The Right to Privacy in the Face of Cyber Attacks (Comparative Study)," Researcher Professor Journal for Legal and Political Studies, Issue 8, December 2007.

- Fatiha Hizam, "Legal Guarantees for Processing Personal Data," Al-Ijtihad Journal for Legal and Economic Studies, Volume 08, Issue 4, 2019.
- Mohammed Al-Eidani, Youssef Zarouk, "Protection of Personal Data in Algeria in Light of Law No. 18/07," Maalim Journal for Legal and Political Studies, Issue 05, December 2018.
- Aisha Ben Qara Mustafa, "Mechanisms for Protecting Personal Data in Algerian Legislation According to the Provisions of Law No. 18-07," Journal of Legal and Political Sciences, Volume 10, Issue 01, April 2019.

E- Seminar papers:

- Samia Shahi Qumurah et al., "Artificial Intelligence Between Reality and Expectation: A Technical and Field Study," Presentation at the International Symposium on Artificial Intelligence: A New Challenge for the Law, November 26-27, 2018, Algeria, Page 5.

F- Websites:

- Osinde A. Osuba, William Wilser IV, "Risks of Artificial Intelligence to Security and the Future of Work," RAND Corporation, WWW.rand.org, 2017.
- Futura, "Artificial Intelligence: What Is It?" https://www.futura-sciences.com/tech/definitions/informatique-intelligence-artificielle-555/.
- International Covenant on Civil and Political Rights, December 16, 1966, published on the website http://hrlibrary.umn.edu/arab/b003.html.
- The Universal Declaration of Human Rights published on the United Nations website: https://www.un.org/ar/universal-declaration-human-rights/index.html.

G- Reports:

- Mohamed El-Hadi El-Souhaili, "Developments in Artificial Intelligence and the Requirements for Protecting Rights and Fundamental Freedoms," Islamic World Organization for Education, Science, and Culture (ISESCO), Legal Affairs Department.