Pak. j. life soc. Sci. (2024), 22(2): 18200-18215 E-ISSN: 2221-7630;P-ISSN: 1727-4915

Pakistan Journal of Life and Social Sciences

www.pjlss.edu.pk

https://doi.org/10.57239/PJLSS-2024-22.2.001329

RESEARCH ARTICLE

The Protection of Personal Data in Algeria: Between Local Challenges and International Standards

CHERIFI Imad[1*], ZERGUINI Radia[2]

[1,2]Lecturer Class A, Faculty of Law and Political Sciences, University of El Oued, Algeria

ARTICLE INFO

Received: Oct 17, 2024

Accepted: Dec 2, 2024

Keywords

Personal Data Protection

Algeria

GDPR

Law No. 18-0

Cybersecurity

International Standard

Data Privacy

Legislative Framework

***Corresponding Author:**

cherifi-imad@univ-eloued.dz

ABSTRACT

The protection of personal data has become a critical issue in the face of the rapid digital transformations. The spread of advanced technologies, such as the internet and artificial intelligence, has increased the collection and exchange of personal data, exposing it to privacy and security risks. In response, many countries have issued legislations to ensure the protection of personal data and regulate its processing to be in line with the international standards. Accordingly, the present study focuses on the importance of personal data protection, examining Algeria's legal framework for safeguarding personal data, its compliance with international standards, and the challenges it faces in practical application. It also explores the enactment of the Law No. 18-07 that is dated on June 10, 2018, concerning the protection of natural persons in the processing of personal data, which aligns with the requirements of the digital age and enhances cybersecurity. Despite Algeria's legal advancements, it still faces a number of challenges, which requires ongoing efforts to ensure compliance and address legal gaps. The study concludes with suggestions for enhancing international cooperation, establishing regional supervisory bodies, and fostering awareness and training to ensure effective protection of personal data in Algeria.

INTRODUCTION

The protection of personal data has become one of the main challenges facing nations in the digital age. The spread of advanced technologies, such as the internet and artificial intelligence, has led to increased collection and exchange of personal data, exposing it to multiple risks related to privacy and security. These developments have prompted countries to adopt certain legislations in order to ensure data protection and regulate its handling in accordance with international standards.

Protecting personal data has significant importance in today's digital era, where personal information is prone to numerous threats from various parties. By understanding the significance of personal data protection, appropriate legislations can be formulated. Hence, a legal framework can be established to prevent the misuse of such data. This includes raising awareness and providing training to ensure that individuals understand their rights to maintain their privacy and to have their personal data processed securely and responsibly.

To achieve this, the Algerian legislator enacted the Personal Data Protection Law under Law No. 18-07 that is dated on June 10, 2018, concerning the protection of natural persons in the field of personal data processing. This law aims to keep pace with the digital technology and harness its benefits while countering cyber security threats and mitigating their risks. This contributes to the country's integration into the digital market, leading to the revitalization of e-commerce, which in turn reflects on the nation's development and prosperity by providing the necessary protection. This enhances citizens' trust in these new transactions.

Therefore, the central issue raised in this topic is: To what extent can the Personal Data Protection Law for natural persons in the field of personal data processing serve as a protective shield against local challenges? And do Algeria's data protection policies comply with international and regional standards?

In this study, we will review the conceptual aspects of personal data, followed by Algeria's efforts in establishing a legal framework for personal data protection. Subsequently, we will address the challenges faced by these efforts and assess the extent to which national legislation aligns with international standards.

2. Concept of Personal Data and Its Importance

2.1 Concept of Personal Data

Personal data encompasses all information pertaining to a specific individual that can be used to identify them, either directly, such as name and address, or indirectly, such as biometric data or financial information.

2.1.2 Concept of Personal Data According to Algerian Law

In Algeria, personal data is regulated under Law No. 18-07 dated June 10, 2018, concerning the protection of natural persons in the processing of such data. According to this law, "personal data" refers to any information, regardless of its medium, related to an identified or identifiable person, herein referred to as the "data subject," either directly or indirectly. This includes reference to an identification number or one or more elements specific to their physical, physiological, genetic, biometric, mental, economic, cultural, or social identity[1]. As per the provisions of the article, personal data encompasses any information related to a specific natural person or one who can be identified directly or indirectly through an identification number or special data such as name, address, email, phone number, or other data that can be used to recognize the person's identity. Examples include: first and last name, biometric ID number of the national identity card and passport, phone number, email address, etc.

2.1.3 Concept of Personal Data According to Tunisian Law

In Tunisian law, Article 4 of the Basic Law concerning the Protection of Personal Data states: "Personal data, for the purposes of this law, means any data regardless of its source or form that makes a natural person identifiable or identifiable in a direct or indirect manner, except for information related to public life or legally considered as such."[2] This definition is similar to that of the Algerian legislator in that it indicates that the information can relate to a person's identity or activities, thereby broadening the concept of personal data to include various aspects related to an individual's daily life.

[1] Article 03 of Law No. 18-07, dated 10/06/2018, concerning the Protection of Natural Persons in the Processing of Personal Data, as published in the Official Gazette of the People's Democratic Republic of Algeria, No. 34, issued on 10/06/2018.

[2] Law No. 63-2004, dated 27/07/2004, concerning the Protection of Personal Data, as published in the Official Gazette of the Tunisian Republic, No. 61, issued on 30/07/2004.

2.1.4 Concept of Personal Data According to the GDPR

According to Article 4 of the General Data Protection Regulation (GDPR)[3], which came into effect in France and the European

Union in 2018: "Personal data" means any information relating to an identified or identifiable natural person ("data subject"); a natural person is considered identifiable if they can be identified, directly or indirectly, in particular by reference to an identifier such as a name, identification number, location data, or an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person[4].

The French (and European under the GDPR) definition is more detailed, specifying particular types of data such as geographic location, biometric, and economic identity, which makes the scope of personal data broader compared to Algerian and Tunisian legislations.

2.1.5 The GDPR's Personal Data Protection Law Derived Its Definition From:

International Human Rights Conventions: Through Article 8 of the European Convention on Human Rights (ECHR), which guarantees the right to respect for private and family life, home, and correspondence, forming the foundation for the concept of personal data protection[5]. Convention 108 of the Council of Europe, adopted in 1981, is the first binding international treaty on the protection of individuals concerning the automated processing of personal data[6].

National Legislations of European Union Countries: The GDPR also draws upon previous national data protection legislations within EU member states, such as the French law "Loi Informatique et Libertés" enacted in 1978. It also references the European Convention on Human Rights (2000), specifically Article 8 of the Charter, which grants individuals the right to protect their personal data[7], and the European Directive 95/46/EC[8], which was the previous foundation for the GDPR, established in 1995 to regulate personal data processing within the European Union. The GDPR replaced this directive to update the rules and keep pace with digital advancements.

2.2 Importance of Protecting Personal Data: The importance of protecting personal data lies in its role in safeguarding individual privacy, preventing unlawful exploitation of information, developing secure services, enhancing trust in the digital environment, and respecting confidential information.

---

[3] The General Data Protection Regulation (GDPR) is a new law that began to be implemented on May 25, 2018, in the European Union countries and the United Kingdom. It is the law that compels internet service providers in Europe to adhere to numerous rules with the aim of protecting user data and providing users with a way to control the data these companies collect about them." See Mohamed El Sayed, "What are GDPR Rules? And How Do They Affect User and Company Privacy?", 2020. Available at: https://tech-echo.com/what-is-gdpr-privacy-rules-summary/.

[4] Art4, the Regulation (EU) 2016/679 (General Data Protection Regulation) in the current version of the OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018 :https://gdpr-info.eu/art-4-gdpr/ .

[5] The European Convention on Human Rights, announced on 04/11/1950 in Rome and ratified on 03/09/1953, amended by Protocols No. 11 and 14, as referenced on the website of the European Court of Human Rights, https://www.echr.coe.int/documents/d/echr/Convention_ARA.

[6] Convention 108+, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, available at the Council of Europe website: https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726.

[7] The European Charter of Human Rights of 2000, available at the Human Rights Library of the University of Minnesota website, at the following link: http://hrlibrary.umn.edu/arab/eu-rights-charter.html.

[8] Directive No. 95/46/EC issued by the European Parliament and the Council on October 24, 1995, concerning the protection of individuals with regard to the processing of personal data and the free movement of such data, available at: https://www.wipo.int/wipolex/ar/legislation/details/13580.

2.2.1 Protecting Privacy: The principle of respecting individual privacy is enshrined in constitutions and legislations as a fundamental right. Protecting privacy enhances individuals' trust in institutions that handle their personal data.

2.2.2 Enhancing Trust in Electronic Transactions: In light of the ongoing developments in the digital sector, providing protection for personal data supports trust in electronic transactions, particularly in e-commerce[9].

2.2.3 Contributing to the Development of Secure Services: Controlling and regulating the processing of personal data contributes to improving services associated with personal information, such as banking services.

2.2.4 Preventing Data Misuse: Legislation related to the protection of personal data helps safeguard data from unlawful exploitation, whether to achieve illegitimate interests or manipulate it, such as in cases of hacking and fraud.

2.2.5 Maintaining Data Confidentiality: Institutions must commit to protecting the confidentiality of personal data and not disclose or share it except with the consent of the data subjects in accordance with applicable legal provisions.

2.2.6 Enhancing Cybersecurity: A robust data protection framework contributes to overall cybersecurity by reducing risks associated with breaches and unauthorized access, which can lead to financial losses and reputational damage.

3 .Legal Framework for the Protection of Personal Data in Algeria

Within Algeria's move towards establishing e-government requirements and fulfilling its international obligations, the legislator has updated and amended the legal system to keep pace with technological advancements. This approach was enshrined in the " The 2020 Constitutional Amendment", where Article 47, Paragraph 4 states: "The protection of individuals in the processing of personal data is a fundamental right"[10].

Additionally, the Penal Code, from Article 303 bis to Article 303 bis 3, includes penalties for anyone who intentionally violates the privacy of individuals[11]. Furthermore, the legislator issued Law No. 15-04 concerning electronic signatures and certification, which stipulates in Article 61 the responsibility of the holder of an electronic certification certificate for the confidentiality of its data[12].

Subsequently, Law No. 18-07 [13]concerning electronic commerce was enacted, wherein Article 11, Paragraph 6 mandates that electronic providers adhere to general sales conditions, emphasizing the

[9] Amina Masyad, "Mechanisms for Protecting Personal Data under Law (18-07)," Journal of the Researcher in Legal and Political Sciences, No. 05, Souk Ahras University, Souk Ahras, Algeria, June 2021, p.104.

[10] Constitution of the People's Democratic Republic of Algeria, 1996, published under Presidential Decree No. 96-438, dated 07/12/1996, as published in the Official Gazette of the People's Democratic Republic of Algeria, No. 76, issued on 08/12/1996, amended by the constitutional revision approved in the referendum of 1st November 2020, as published in the Official Gazette of the People's Democratic Republic of Algeria under Presidential Decree No. 20-442, dated 30/12/2020, Official Gazette No. 82, issued on 30/12/2020.

[11] Order No. 66-156, dated 08/06/1966, concerning the Penal Code, as published in the Official Gazette of the People's Democratic Republic of Algeria, No. 49, issued on 11/06/1966, amended and supplemented.

[12] Law No. 15-04, dated 01/02/2015, concerning the general rules for electronic signatures and certification, as published in the Official Gazette of the People's Democratic Republic of Algeria, No. 06, issued on 10/02/2015.

[13] Law No. 18-05, dated 10/05/2018, concerning electronic commerce, as published in the Official Gazette of the People's Democratic Republic of Algeria, No. 28, issued on 16/05/2018.

protection of personal data, maintaining its confidentiality, and prohibiting its use for unauthorized purposes[14].

3.1 Law No. 18-07 Concerning the Protection of Personal Data

With the enactment of Law No. 18-07 concerning electronic commerce in Algeria, a set of rights is granted to natural persons regarding the processing of personal data to ensure the protection of their privacy and the safeguarding of their data in the digital environment. The following are the key rights guaranteed by the law:

3.1.1 Right to Access Personal Data

A natural person has the right to know the data collected about them and how it is used by the electronic provider or the relevant authority.

3.1.2 Right to Prior Consent

The law requires explicit consent from the individual before collecting or processing their personal data, ensuring control over how this data is used. In cases where the data subject is incapacitated or partially incapacitated, consent is regulated in accordance with general legal provisions[15].

Consent from the data subject is not required for the processing of personal data in the following cases[16]:

- Legal Obligation: If the processing is necessary to comply with a legal obligation imposed on the data subject or the data controller.
- Protection of Life: When processing is necessary to protect the life of the data subject.
- Contract Execution: If processing is necessary for the performance of a contract to which the data subject is a party or to take preparatory measures at their request.
- Protection of Vital Interests: In cases where the person is physically or legally unable to express their consent.
- Public Interest Tasks: When processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
- Legitimate Interests: If the processing aims to achieve legitimate interests of the data controller or the recipient, considering the rights and fundamental freedoms of the data subject.

The data subject has the right to withdraw their consent at any time without affecting the lawfulness of processing based on prior consent.

3.1.3 Right to Rectification and Modification

If the collected data is incorrect or incomplete, the individual has the right to request its modification or correction to ensure the accuracy of the information. The data subject is entitled to obtain, free of charge from the data controller, the following[17]:

-Updating, correcting, deleting, or closing personal data that are non-compliant with the law due to inaccuracy or unlawful processing. The controller is obligated to make the required corrections free of charge within 10 days of notification. In case of refusal or no response, the data subject can submit a request to the national authority, which will investigate and take necessary actions. The data

[14] Yazid Boujlet and Abdelrahman Fatanasi, "Administrative and Criminal Protection in the Field of Personal Data Processing in Light of Law 18-07," Journal of Legal and Political Research, Vol. 06, No. 02, Mohamed Seddik Ben Yahia University, Jijel, December 2021, p. 56.

[15] Article 07 of Law No. 18-07 concerning the Protection of Natural Persons in the Processing of Personal Data.

[16] Ibid.

[17] Article 35 of Law No. 18-07 concerning the Protection of Natural Persons in the Processing of Personal Data.

controller must inform the entities that received the personal data of any changes or corrections made, unless it is impossible.

The heirs of the data subject can also benefit from these rights.

3.1.4 Right to Object to Processing

The law grants individuals the right to object, for legitimate reasons, to the processing of their personal data, especially if the purpose is promotional or commercial, whether by the current or future data controller.

However, this right does not apply if the processing is carried out in response to a legal obligation or if this right is explicitly excluded by the document that allows the processing[18].

3.1.5 Right to Erasure (Right to be Forgotten)

Individuals have the right to request the deletion of their data once the purpose for which it was collected has been fulfilled or if it has been used unlawfully.

3.1.6 Right to Data Confidentiality

The data controller must implement appropriate technical and organizational measures to protect personal data from accidental or unlawful loss, destruction, or alteration, as well as from unauthorized access or disclosure[19]. Additionally, data protection must be ensured during its transmission across networks, ensuring that all operations are conducted in accordance with the law. Security measures should be proportionate to the potential risks and the type of data to be protected to ensure an adequate level of security.

According to Article 11, Paragraph 6 of the law, the electronic provider must comply with protecting personal data, maintaining its confidentiality, and not using it for purposes other than those agreed upon.

3.1.7 Right to Notification in Case of Data Breach

The law obliges the relevant authorities to notify individuals in the event of a security breach or data leakage concerning their personal data.

4 .Regulatory Framework for the Protection of Personal Data in Algeria:

4 .1 -The National Authority for the Protection of Personal Data:

This authority was established to monitor and ensure compliance with the law regarding the processing of personal data, ensuring that both public and private institutions adhere to the principles of data collection and usage. The Algerian legislator outlined this authority in Law No. 18-07 concerning the protection of personal data in Article 22: "An independent administrative authority for the protection of personal data shall be established under the President of the Republic, hereinafter referred to as the 'National Authority,' with its headquarters located in Algiers. The National Authority shall have legal personality and financial and administrative independence. Its budget is included in the national budget and is subject to financial control in accordance with applicable legislation. The National Authority shall adopt its internal regulations, which specify, in particular, its organization and operation, and shall be approved by it "[20].The National Authority ensures the respect of human dignity and the right to privacy during the processing of personal data.

[18] Article 38 of Law No. 18-07 concerning the Protection of Natural Persons in the Processing of Personal Data.
[19] Ibid.
[20] Article 22 of Law No. 18-07 concerning the Protection of Natural Persons in the Processing of Personal Data.

It is an "independent administrative authority"[21] that enjoys legal personality and financial and administrative independence. Its headquarters are located in the Wilaya of Algiers (Haidara Municipality), and it consists of 16 members, including its President, appointed by Presidential Decree No. 22-187 dated May 18, 2022[22]. The President and members of the authority were installed on August 11, 2022[23].

4.2 - Organization of the National Authority for the Protection of Personal Data

The organizational structure of the National Authority for the Protection of Personal Data consists of a President and a group of members, along with an executive secretariat containing study managers and heads of studies. The structure is divided into three main directorates:

- Legal Affairs Directorate: This includes a sub-directorate for legal affairs, a sub-directorate for disputes, and a sub-directorate for compliance.
- -Communication and Information Systems Directorate: This includes a sub-directorate for information and communication, a sub-directorate for software study and development, and a sub-directorate for managing IT systems.
- General Administration Directorate: This includes a sub-directorate for human resources and training, and a sub-directorate for finance and resources[24].

3.4 - Tasks of the National Authority for the Protection of Personal Data

The National Authority for the Protection of Personal Data is responsible for overseeing compliance with the provisions of Law No. 18-07 regarding the processing of personal data and ensuring that the use of information and communication technologies does not negatively affect individuals' rights and public freedoms, while maintaining the sanctity of private life. Its duties include[25]:

Issuing licenses and receiving declarations related to the processing of personal data.

Informing all concerned individuals and data controllers of their rights and obligations.

Providing consultations to individuals and entities involved in personal data processing or conducting studies or experiments that may lead to such processing.

Receiving complaints and grievances regarding the processing of personal data and informing the complainants of its decisions.

Issuing licenses for the transfer of personal data abroad, in accordance with the conditions specified in the law.

Issuing orders for necessary modifications to protect personal data under processing.

---

[21] Definition of the National Authority, available on the website of the National Authority for the Protection of Personal Data, https://anpdp.dz.

[22] Presidential Decree No. 22-187, dated 18/05/2022, concerning the appointment of the President and members of the National Authority for the Protection of Personal Data, as published in the Official Gazette of the People's Democratic Republic of Algeria, No. 35, issued on 24/05/2022.

[23] National Authority for the Protection of Personal Data, Installation of the President and Members of the National Authority, available on the website of the National Authority for the Protection of Personal Data, https://anpdp.dz/fr/2022/08/11/installation-du-president-et-des-membres-de-lautorite-nationale-de-protection-des-donnees-a-caractere-personnel/.

[24] - Presidential Decree No. 23-73, dated 14/02/2023, specifying the duties of the Executive Secretariat of the National Authority for the Protection of Personal Data and the procedures for its organization and operation, as published in the Official Gazette of the People's Democratic Republic of Algeria, No. 10, issued on 15/02/2023.

[25] Duties of the National Authority, available on the website of the National Authority for the Protection of Personal Data: https://anpdp.dz.

In accordance with the provisions of Article 75 of Law No. 18-07 concerning the protection of personal data, which states: "Under the penalty of sanctions provided for in Article 56 of this law, individuals engaged in personal data processing activities at the time of the issuance of this law must comply with its provisions within a period of one year from the date of the installation of the National Authority." As mentioned above, the National Authority for the Protection of Personal Data was installed on August 11, 2022, and compliance with the provisions of the law by individuals engaged in personal data processing activities began on August 10, 2023.

5 .International and Regional Standards for Personal Data Protection

5.1 - International Standards for Personal Data Protection

5.1.1 - General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a set of European laws adopted on April 27, 2016, and came into force on May 25, 2018. The regulation aims to enhance the protection of personal data for European citizens and unify data protection laws across all EU member states, facilitating the movement of information and e-commerce within the European market.

5.1.2 - Objectives of the Regulation

- Protection of Rights: The regulation aims to protect individuals' rights and ensure that their data is used transparently and securely.
- Harmonization of Laws: The regulation seeks to harmonize the laws concerning the protection of personal data across EU countries to facilitate e-commerce and reduce legal barriers.
- Increased Transparency: Institutions are required to clarify how personal data is collected, processed, and stored.
- Building Trust: By ensuring the secure handling of personal data, the regulation fosters trust among citizens, encouraging digital interaction and e-commerce.

3.1.5 - Basic Principles of the General Data Protection Regulation (GDPR)

The processing of personal data must be characterized by [26]:

Lawfulness, Fairness, and Transparency: Data must be processed in a transparent, lawful, and fair manner.

Data Collection Limitation: Data collection must be specific, explicit, and legitimate, and cannot be processed in a manner incompatible with these purposes.

Data Minimization: Only the necessary data should be collected to achieve the processing purposes.

Accuracy: Data must be accurate and up-to-date, with steps taken to correct inaccurate or incomplete data promptly.

Storage Limitation: Personal data should be kept only for as long as necessary to fulfill the purposes for which it was collected.

Integrity and Confidentiality: Data must be processed in a way that ensures its protection from unauthorized processing, loss, or alteration.

Accountability: Institutions must comply with the GDPR's fundamental principles and implement appropriate measures to ensure compliance.

[26] Article 05 of the General Data Protection Regulation (GDPR) Principles Relating to the Processing of Personal Data Available at: https://gdpr-info.eu/art-5-gdpr/.

5.1.4 - Rights of Individuals under the GDPR

The regulation includes several rights for individuals whose personal data is being processed, including:

5.1.4.1 -**Right of Access**: The data subject has the right to obtain confirmation of whether their personal data is being processed and access information about the data, including its purpose, retention period, and the right to request correction or deletion[27].

5.1.4.2 **Right to Rectification**: Individuals can request the correction of inaccurate or incomplete personal data[28].

5.1.4.3 **Right to Erasure (Right to be Forgotten):** Individuals can request the deletion of their personal data under certain circumstances[29].

5.1.4.4 Right to Restrict Processing: The data subject can request the restriction of the processing of their personal data in specific situations[30].

5.1.4.5 Notification: Individuals must be notified of any erasure, correction, or restriction of their personal data[31].

5.1.4.6 Right to Data Portability: Individuals can request the transfer of their personal data to another entity in a structured, commonly used, and machine-readable format[32].

5.1.4.7 Right to Object: Individuals can object to the processing of their personal data in certain circumstances for specific reasons[33].

5.1.5 - Obligations of Data Processing Entities under the GDPR

5.1.5.1 Obtaining Explicit Consent: Organizations must obtain explicit consent from individuals before collecting or processing their personal data.

5.1.5.2 Data Protection: Organizations must implement appropriate technical and organizational measures, such as data anonymization, to ensure the protection and minimization of data, integrating necessary safeguards to meet GDPR requirements and protect individuals' rights. [34]

5.1.5.**3 Notifying Supervisory Authority of Data Breaches**: Organizations must inform the supervisory authority of any data breaches affecting personal data within 72 hours of discovery[35].

5.1.5.4 Data Protection Impact Assessment: Organizations should conduct assessments to identify potential risks to individuals' privacy and take necessary measures to mitigate these risks effectively[36].

5.1.5.5 **Appointment of a Data Protection Officer**: In certain cases, organizations must appoint a Data Protection Officer (DPO) to ensure compliance with the GDPR and to oversee the organization's data protection activities[37].

---

[27] Article 15 of the General Data Protection Regulation (GDPR).
[28] .Ibid, Article 16.
[29] .Ibid, Article 17.
[30] .Ibid, Article 18.
[31] Article 19 of the General Data Protection Regulation (GDPR).
[32] .Ibid, Article 20.
[33] .Ibid, Article 21.
[34] .Ibid, Article 25.
[35] .Ibid, Article 33.
[36] .Ibid, Article 35.
[37] .Ibid, Article 37.

5.1.5.**6 Prior Consultation**: When a data protection impact assessment indicates high risks to individuals' privacy, organizations must consult the supervisory authority before proceeding with the data processing.

5.1.5.7 Training and Awareness: Organizations must train their employees on GDPR requirements and the importance of personal data protection.

5.2 - Regional (African) Standards for the Protection of Personal Data

5.2.1-The African Convention on Personal Data Protection and Cybersecurity[38]: The African Union adopted the "African Convention on Personal Data Protection and Cybersecurity," which aims to establish a common framework among member states to ensure data protection. This Convention represents a significant legal framework at the continental level, aiming to protect personal data and enhance cybersecurity in African countries. It was adopted by the African Union to promote individuals' rights to privacy and data protection and to strengthen countries' abilities to address cyber threats.

5.2.2 - Objectives of the Convention

-Personal Data Protection: To provide a legal framework for the protection of individuals' personal data and ensure their rights related to privacy.

-Enhancing Cybersecurity and Combating Crime: Each African Union member state is committed to establishing a national policy to protect cyberspace, following a national strategy that includes legislative reforms to criminalize privacy breaches. All procedural measures must be taken to monitor and prosecute anyone who violates the legislation[39]. Additionally, there should be awareness-raising efforts to inform the public and institutions about technology-related threats, as well as training and education on necessary preventive measures to combat cyber threats and protect systems and information[40].

-Harmonization of Legislation: To work on unifying legislation, laws, and policies related to the protection of personal data and cybersecurity across all member states of the Convention.

-Governance of Cybersecurity: Each member state commits to taking all necessary measures to establish an appropriate institutional mechanism aimed at achieving effective cybersecurity governance, which contributes to enhancing the response to challenges and threats related to cybersecurity[41].

-International Cooperation: To strengthen cooperation among member states in the field of data protection and security by establishing institutions to exchange information on cyber threats, leveraging the commitment of signatory states to use existing international cooperation mechanisms to respond to security threats, and improving cybersecurity.

5.2.3 - African Basic Principles for Personal Data Protection and Cybersecurity

Transparency: Personal data can only be processed (collected and used) with the consent of the concerned individual, except in certain necessary cases provided for by the Convention[42].

---

[38] African Union Convention on Cyber Security and Personal Data Protection, Date of Adoption: June 27, 2014, Date of last signature: May 11, 2020, Available on the website: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[39] Chapter Three (Articles 24-25-26) of the African Convention on Personal Data Protection and Cybersecurity

[40] Meriem Lokhal, "Reading in the African Union Convention on Cybersecurity and the Protection of Personal Data of 2014," Journal of Legal and Economic Studies, Vol. 4, Issue 3, University Center of Brika, 2021, p. 664.

[41] Article 27 of the African Convention on Personal Data Protection and Cybersecurity.

[42] Article 13, Principle 01, of the African Convention on Personal Data Protection and Cybersecurity.

Accountability: Making entities responsible for data processing accountable for the protection of personal data.

Purpose Limitation: Personal data collection must have a clear, legitimate purpose and be limited to what is necessary to achieve the specified purposes[43].

Individual Rights: This Convention grants clear rights to individuals, including the right to be provided with information, such as the identity and purposes of processing, the right to view their data, and the right to access information (enabling them to know which information they can object to processing). These rights also include the right to object to data processing, as well as the right to correct and delete their data[44].

Confidentiality and Security: The processing of personal data must be confidential, especially when transferring such data over communication networks[45].

Accuracy: Collected data must be accurate, up-to-date when necessary, and incorrect data must be deleted or corrected, considering the purposes for which it was collected[46].

Cooperation and Coordination among Member States of the Convention: To enhance cooperation among African countries in addressing challenges related to data protection and cybersecurity.

5.2.4 - Importance of the African Convention on Personal Data Protection and Cybersecurity
The importance of the Convention lies in fostering trust in digital transactions by providing a clear legal framework that protects personal data. It also contributes to safeguarding individuals' privacy in the digital age, offering effective mechanisms to address growing cybersecurity challenges in African countries.

6 .Compatibility of Algeria with International Standards

Algeria has sought to align with international and regional agreements and legislative texts in the field of personal data protection by issuing a series of legislations, such as the law on e-commerce, the law on general rules related to electronic signatures and certification[47], and most recently, the Personal Data Protection Law[48]. Through the latter, Algeria aims to achieve compatibility with international standards, particularly the "General Data Protection Regulation (GDPR)." Some of the key aspects of this alignment include:

6.1 - Rights Contributing to Enhancing Individuals' Trust in the Processing of Their Personal Data

These rights ensure that data is processed in a manner that respects privacy, including[49]:

6.1.1 - The Right to Prior Consent: Personal data may only be processed with the explicit consent of the individual concerned.

6.1.2 - **Transparency (Right to Information):** Prior and explicit notification must be provided to every person whose data is collected by the data controller.

[43] .Ibid, Article 13, Principle 03.
[44] .Ibid, Articles 17-18-19.
[45] .Ibid, Article 13, Principle 06.
[46] .Ibid, Article 13, Principle 04.
[47] Law 18-05, related to Electronic Commerce. And Law 15-04, related to the General Rules for Electronic Signatures and Certification.
[48] Law 18-07, on the Protection of Natural Persons in the Processing of Personal Data, previous source.
[49] Articles 7, 32, 34, 35, and 36 of Law 18-07, , related to the Protection of Natural Persons in the Processing of Personal Data.

6.1.3-**Right of Access:** The individual has the right to access their personal data and know whether it has been processed and for what purpose.

6.1.4-**Right to Object:** The individual has the right to object to the processing of their personal data.

6.1.5-**Right to Be Forgotten**: Individuals are granted the right to update, correct, and delete their personal data.

2.6 - Establishment of the National Authority for the Protection of Personal Data

As stipulated in Chapter Three of Law 18-07 on the protection of natural persons in the processing of personal data, the National Authority was established in 2022. The Authority ensures the respect of human dignity and the right to privacy during the personal data processing.

Despite the legal and regulatory framework established by the legislator for the protection of personal data, the practical application of these laws still faces significant challenges that require continuous efforts to ensure full compliance and avoid legal gaps. This includes several key areas that must be focused on to achieve the desired objectives of the legislation, including:

Ongoing Training and Awareness Programs: Continuous training for employees at all levels to ensure they deeply understand the requirements of data protection and how to apply them in their daily tasks. Individuals must also be made aware of their rights and duties regarding their personal data, promoting a culture of respect for privacy and legal compliance[50].

Continuous Development of Systems: The continuous development of systems through modern technologies that ensure protection from breaches, with the consistent use of advanced data encryption technologies to protect data during storage and transmission.

Creation of an Independent Regional (African) Data Protection Authority: To coordinate between data protection authorities, similar to the European Union's model, which operates through the European Data Protection Board (EDPB)[51].

Also, the establishment of an independent regional (African) supervisory authority, whose primary objective is to oversee and monitor to ensure that institutions and bodies respect the right to privacy and data protection when processing personal data and developing new policies, similar to what the European Union has done through the creation of the European Data Protection Supervisor (EDPS) [52], The duties and powers of the Data Protection Supervisor as a supervisory

[50] Commission Nationale de l'Informatique et des Libertés, Les droits pour maîtriser vos données personnelles, Disponible sur le site suivant : https://www.cnil.fr/fr/mes-demarches/les-droits-pour-maitriser-vos-donnees-personnelles.

[51] The European Data Protection Board (EDPB) is an independent agency of the European Union aimed at ensuring the consistent application of the General Data Protection Regulation (GDPR) and enhancing cooperation between data protection authorities across the European Union. On May 25, 2018, the European Data Protection Board was established. Available on the Wikipedia website, the free encyclopedia: https://en.wikipedia.org/wiki/European_Data_Protection_Board.

[52] The EDPS (European Data Protection Supervisor) is an independent supervisory authority whose primary objective is to monitor and ensure that European institutions and bodies respect the right to privacy and data protection when processing personal data and developing new policies. Available at: https://commission.europa.eu/law/law-topic/data-protection_en.
Its mandate includes monitoring and ensuring the protection of personal data and privacy when EU institutions and bodies process individuals' personal information, and providing advice to EU institutions and bodies on all matters related to personal data processing, either upon request or on its own initiative. In particular, it is consulted by the European Commission regarding proposals for legislation and international agreements. Available at: https://www.edps.europa.eu/about-edps_en.

authority are: supervision, consultation, and cooperation with other data protection authorities in Europe[53].

7 .CONCLUSION

The protection of personal data in Algeria represents a central issue in light of the rapid digital transformations. Despite the efforts made to develop the legal framework, there are still challenges hindering the actual application of these laws. Achieving effective data protection requires cooperation among various parties, including the government, the private sector, and civil society, as well as enhancing alignment with international standards, through taking appropriate steps that will enable Algeria to build an integrated data protection system that contributes to enhancing trust between individuals and institutions, and protects their privacy in the digital age.

From the study, we have concluded several findings, the most significant of which are:

The Algerian legislator defined personal data as: "Any information, regardless of its medium, related to a person who is identified or can be identified, referred to hereinafter as 'the data subject', directly or indirectly, especially by reference to an identification number or one or more elements specific to their physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity." This definition is not much different from other international and regional definitions.

Among the rights guaranteed by Law 18-07 on the protection of personal data in Algeria are: the right to access personal data, the right to prior consent, the right to correction and modification, the right to object to processing, and the right to be forgotten.

The National Authority for the Protection of Personal Data was established in Algeria. This body is responsible for monitoring and ensuring compliance with the law regarding personal data processing and ensuring that public and private institutions adhere to the principles of data collection and usage. It consists of 16 members, including its president, appointed by Presidential Decree No. 22-187 dated May 18, 2022, and inaugurated on August 11, 2022. It resumed its activities as stipulated by Law 18-07 on the protection of natural persons in the processing of personal data, and Presidential Decree No. 23-73 dated February 14, 2023, which defines the tasks of the executive secretariat of the National Authority for the Protection of Personal Data and its organization and operation procedures.

Algeria has sought to align with international and regional agreements and legislative texts in the field of personal data protection by issuing a series of legislations such as the law on e-commerce and the law on general rules related to electronic signatures and certification, with the latest being the Law on Personal Data Protection.

Algeria has sought to achieve compatibility with international standards through this law, especially with the "General Data Protection Regulation (GDPR)," by aligning with the African Convention on Personal Data Protection and Cybersecurity. Some of the manifestations of this alignment in the field of individual rights in the protection of personal data include: the right to prior consent, transparency (the right to be informed), the right of access, the right to object, and the right to be forgotten.

Despite the legal and regulatory framework established by the legislator for personal data protection, the practical implementation of these laws continues to face challenges that require sustained efforts to ensure full compliance and close any legal gaps. Key areas of focus are necessary to achieve the objectives of the legislation, including:

[53] Wikipedia website, European Data Protection Supervisor, available at: https://en.wikipedia.org/wiki/European_Data_Protection_Supervisor.

Intensifying training sessions for employees at all levels to understand the importance of data protection.

Conducting awareness campaigns for citizens regarding their rights and duties concerning their personal data.

Continuously developing systems and regularly updating technologies to keep up with data protection techniques against breaches.

Suggestions:

Enhance international cooperation by joining international agreements and activating the outcomes of ratified regional agreements related to data protection, in order to benefit from global expertise.

Establish a regional supervisory authority similar to the European approach with the creation of the European Data Protection Supervisor (EDPS), an independent supervisory body whose primary goal is to monitor and ensure that European institutions and bodies respect privacy and data protection rights when processing personal data.

Increase public awareness by launching awareness campaigns to inform citizens of their rights in data protection and the importance of exercising caution when providing personal data to any entity.

Empower human resources and update infrastructure by providing advanced technical resources and training cybersecurity specialists to ensure effective and comprehensive data protection.

Encourage the private sector to integrate data protection policies by adopting precise and modern techniques for data security, offering incentives for institutions that implement stronger protection measures, and penalizing those who violate the legal provisions governing the protection of personal data.

REFERENCES

-THE Constitution

1-Constitution of the People's Democratic Republic of Algeria, 1996, published under Presidential Decree No. 96-438, dated 07/12/1996, as published in the Official Gazette of the People's Democratic Republic of Algeria, No. 76, issued on 08/12/1996, amended by the constitutional revision approved in the referendum of 1st November 2020, as published in the Official Gazette of the People's Democratic Republic of Algeria under Presidential Decree No. 20-442, dated 30/12/2020, Official Gazette No. 82, issued on 30/12/2020.

Legal texts:

A/ Legislative texts

2-Order No. 66-156, dated 08/06/1966, concerning the Penal Code, as published in the Official Gazette of the People's Democratic Republic of Algeria, No. 49, issued on 11/06/1966, amended and supplemented.

3-Law No. 63-2004, dated 27/07/2004, concerning the Protection of Personal Data, as published in the Official Gazette of the Tunisian Republic, No. 61, issued on 30/07/2004.

4-Law No. 18-05, dated 10/05/2018, concerning electronic commerce, as published in the Official Gazette of the People's Democratic Republic of Algeria, No. 28, issued on 16/05/2018.

5-Law No. 18-07, dated 10/06/2018, concerning the Protection of Natural Persons in the Processing of Personal Data, as published in the Official Gazette of the People's Democratic Republic of Algeria, No. 34, issued on 10/06/2018.

B/ Regulatory texts:

6-Presidential Decree No. 22-187, dated 18/05/2022, concerning the appointment of the President and members of the National Authority for the Protection of Personal Data, as published in the Official Gazette of the People's Democratic Republic of Algeria, No. 35, issued on 24/05/2022.

7- Presidential Decree No. 23-73, dated 14/02/2023, specifying the duties of the Executive Secretariat of the National Authority for the Protection of Personal Data and the procedures for its organization and operation, as published in the Official Gazette of the People's Democratic Republic of Algeria, No. 10, issued on 15/02/2023.

Scientific articles:

8- Amina Masyad, "Mechanisms for Protecting Personal Data under Law (18-07)," Journal of the Researcher in Legal and Political Sciences, No. 05, Souk Ahras University, Souk Ahras, Algeria, June 2021.

9- Meriem Lokhal, "Reading in the African Union Convention on Cybersecurity and the Protection of Personal Data of 2014," Journal of Legal and Economic Studies, Vol. 4, Issue 3, University Center of Barika, 2021.

10-Yazid Boujlet and Abdelrahman Fatanasi, "Administrative and Criminal Protection in the Field of Personal Data Processing in Light of Law 18-07," Journal of Legal and Political Research, Vol. 06, No. 02, Mohamed Seddik Ben Yahia University, Jijel, December 2021.

Websites:

11-National Authority for the Protection of Personal Data, Installation of the President and Members of the National Authority, available on the website of the National Authority for the Protection of Personal Data, https://anpdp.dz/fr/2022/08/11/installation-du-president-et-des-membres-de-lautorite-nationale-de-protection-des-donnees-a-caractere-personnel/.

12-Mohamed El Sayed, "What are GDPR Rules? And How Do They Affect User and Company Privacy?", 2020. Available at: https://tech-echo.com/what-is-gdpr-privacy-rules-summary/.

the Regulation (EU) 2016/679 (General Data Protection Regulation) in the current version of the OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018 :https://gdpr-info.eu/art-4-gdpr/ .

13-The European Convention on Human Rights, announced on 04/11/1950 in Rome and ratified on 03/09/1953, amended by Protocols No. 11 and 14, as referenced on the website of the European Court of Human Rights, https://www.echr.coe.int/documents/d/echr/Convention_ARA.

14- Convention 108+, the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, available at the Council of Europe website: https://rm.coe.int/convention-108-convention-pour-la-protection-des-personnes-a-l-egard-d/16808b3726.

15-The European Charter of Human Rights of 2000, available at the Human Rights Library of the University of Minnesota website, at the following link: http://hrlibrary.umn.edu/arab/eu-rights-charter.html.

16-Directive No. 95/46/EC issued by the European Parliament and the Council on October 24, 1995, concerning the protection of individuals with regard to the processing of personal data and the free movement of such data, available at: https://www.wipo.int/wipolex/ar/legislation/details/13580.

17- African Union Convention on Cyber Security and Personal Data Protection, Date of Adoption: June 27, 2014, Date of last signature: May 11, 2020, Available on the website: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

18-The European Data Protection Board (EDPB) is an independent agency of the European Union aimed at ensuring the consistent application of the General Data Protection Regulation (GDPR) and enhancing cooperation between data protection authorities across the European Union. On May 25, 2018, the European Data Protection Board was established. Available on the Wikipedia website, the free encyclopedia: https://en.wikipedia.org/wiki/European_Data_Protection_Board.

19-Commission Nationale de l'Informatique et des Libertés, Les droits pour maîtriser vos données personnelles, Disponible sur le site suivant : https://www.cnil.fr/fr/mes-demarches/les-droits-pour-maitriser-vos-donnees-personnelles.

20-The European Data Protection Board (EDPB) is an independent agency of the European Union aimed at ensuring the consistent application of the General Data Protection Regulation (GDPR) and enhancing cooperation between data protection authorities across the European Union. On May 25, 2018, the European Data Protection Board was established. Available on the Wikipedia website, the free encyclopedia: https://en.wikipedia.org/wiki/European_Data_Protection_Board.

21-Wikipedia website, European Data Protection Supervisor, available at: https://en.wikipedia.org/wiki/European_Data_Protection_Supervisor.