E.ISSN: 2661-7404 Academic Journal of Legal and Political Researchs P.ISSN:2571-9971
Year: 2026 Vol : 10 No : 02 Page : 243 - 251

PROTECTING PERSONAL DATA AS AN ADMINISTRATIVE OBLIGATION IN A DIGITAL ENVIRONMENT

Imene Ouahrani *
University of Abu Bakr Belkaid - Tlemcen
(Algeria)
imene.ouahrani@univ-tlemcen.dz

Received: 15- 06- 2026 **Accepted: 15- 08- 2026** **Published: 22- 09- 2026**

Abstract:

The protection of personal data has become a fundamental administrative obligation in the digital age, driven by the expansion of information and communication technologies and e-government services. Public administrations collect and process significant amounts of personal information, requiring effective safeguards against unauthorized access, disclosure, and cyber threats. This obligation is grounded in the protection of privacy and adherence to principles such as legality, transparency, purpose limitation, and data minimization. In Algeria, legislative reforms have reinforced personal data protection, seeking to balance digital transformation with the preservation of fundamental rights and freedoms while enhancing public trust in digital administration.

Keywords: Personal Data Protection; Digital Environment□□Administrative Obligation; Privacy Rights; Law No. 25-11.

Introduction

Technological advancements and the digital transformation of public administration have led to an increasing reliance on electronic means for collecting, processing, and storing data, making personal data one of the most critical resources on which modern administration relies to carry out its functions. However, this development has been accompanied by an increase in privacy-related risks, such as cyberattacks, unauthorized data leaks, and the misuse of personal information.

* **Corresponding author**

E.ISSN: 2661-7404 Academic Journal of Legal and Political Researchs P.ISSN:2571-9971
Year: 2026 Vol : 10 No : 02 Page : 243 - 251

Consequently, the protection of personal data has become an administrative obligation requiring the administration to take the legal, regulatory, and technical measures necessary to ensure that individuals' rights are respected in an evolving digital environment.

This leads us to the following question: To what extent has management succeeded in fulfilling its commitment to data protection in the context of digital transformation?

Objectives of the Study:

This study aims to define the legal framework for the protection of personal data in the digital environment by analyzing the relevant legal texts, assessing the effectiveness of such protection, and proposing ways to improve it.

Methodology:

A descriptive-analytical approach was adopted, involving the presentation and analysis of national legal texts, supplemented by a comparative approach where appropriate.

To further explore this topic, we have decided to divide our study into two main sections: the definition of personal data under Algerian law (Section 1), and (Section 2), which addresses the administrative obligations regarding the protection of personal data.

THE FIRST TOPIC: DEFINITION OF PERSONAL DATA UNDER ALGERIAN LAW

In the age of digitalization and the increasing use of information and communication technology, personal data has become a valuable resource used in many fields, such as management, healthcare, commerce, education, security, and others.

Given this widespread use, there is a clear need for a legal and regulatory framework that ensures the protection of privacy and governs how such data is collected and processed.

FIRST REQUIREMENT: DEFINITION OF PERSONAL DATA

First and foremost, the Algerian legislature has enshrined legal protection for individuals' privacy in several laws, including:

Firstly: The 2020 Constitution: In this context, Article 47 of the Constitution[1] was explicitly established to protect individuals when their personal data is processed, recognizing this as a fundamental constitutional right no less important than other public rights and freedoms, thereby reflecting the Algerian state's commitment to protecting the privacy of its citizens.

Secondly: Decree No. 75-58, which incorporates the Civil Code[2], provides in Article 48 as follows: "Any person who has suffered an unlawful infringement of a right inherent to his or her person may seek an injunction to stop such infringement and compensation for any damage suffered".

Thirdly: The legislature has also criminalized any infringement of personal data in the Penal Code under Articles 394 bis through 394 bis 7[3].

However, these general provisions cannot cover breaches involving automatically processed personal data, particularly in light of technological advances. Although telecommunications were regulated in 2000 under Law No. 2000-03, the law did not address automatically processed personal data[4].

For its part, Law No. 09-04 on specific rules for the prevention and combating of crimes related to information and communication technology[5], defines information data as "any presentation of facts, information, or concepts in a form suitable for processing within an information system, including the appropriate software that enables the information system to perform its function." It specifies the crimes applicable to such data without addressing automatically processed personal data or criminalizing attacks against it.

E.ISSN: 2661-7404 Academic Journal of Legal and Political Researchs P.ISSN:2571-9971
Year: 2026 Vol : 10 No : 02 Page : 243 - 251

The same applies to Law No. 18-04[6], which establishes rules governing postal and electronic communications and repealed Law No. 2000-03; it did not define "personal data," but merely required that the privacy of subscribers and their personal data be protected in service provision regulations.

Law No. 18-07 of June 10, 2018[7], is considered the first law in Algeria dedicated to the protection of natural persons with regard to the processing of personal data; therefore, it pays particular attention to defining the concepts and terminology it contains. It should be noted that the aforementioned law was amended by Law No. 25-11 dated July 24, 2025.

Article 2 defines personal data as follows: " Personal data means any information, regardless of its medium, relating to an identified or identifiable natural person; the data subject is referred to below as the person concerned, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, genetic, biometric, psychological, economic, social, or cultural identity ".

We therefore conclude that the Algerian legislature has based its definition of personal data on several fixed and variable characteristics of an individual that distinguish him or her from others[8], with the aim of protecting individuals from any infringement of their privacy and the rights inherent to their personality in cyberspace. This definition was inspired by comparative legal texts, such as French legislation[9].

SECOND REQUIREMENT: TYPES OF PERSONAL DATA

Personal data is typically classified into several specific categories in the field of data protection, the most important of which are:

Firstly: General Personal Information:

Including first and last name, mailing address and email address, personal photos, marital status, resume, date of birth, phone number, Social Security number, national ID number, passwords, and bank account information.

Secondly: Sensitive Personal Data:

This refers to data whose disclosure could lead to discrimination, and includes the following:

1- Sensitive Data:

This refers to personal data that reveals a person's ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership.

2- Genetic Data:

Law No. 18-07, as amended and supplemented, establishes that genetic data is sensitive information and defines it as "all data relating to the genetic characteristics of a person or several related persons".

3- Health-Related Information:

A person's health condition, medical care, and treatment are among their most private matters; sometimes, falling ill may lead to withdrawal from public life and estrangement from family and relatives. If a person is ill and in such a difficult situation, it is all the more impermissible to publish or broadcast news of their illness or to photograph them while they are bedridden without their explicit consent[10], in accordance with the legal provisions establishing liability for such conduct[11].

Consequently, the Algerian legislature has classified health information as sensitive data subject to protection, defining it in Article 3 of Law No. 18-07, as amended and supplemented, as follows: "Information relating to the physical or mental condition of the person concerned, including genetic data".

E.ISSN: 2661-7404 Academic Journal of Legal and Political Researchs P.ISSN:2571-9971
Year: 2026 Vol : 10 No : 02 Page : 243 - 251

THE SECOND TOPIC: ADMINISTRATIVE COMMITMENT TO THE PROTECTION OF PERSONAL DATA

In the course of going about their daily business, individuals come into contact with and interact with various government agencies, which retain certain information in exchange for the services they provide.

FIRST REQUIREMENT: MANIFESTATIONS OF ADMINISTRATIVE COMMITMENT TO THE PROTECTION OF PERSONAL DATA

The protection of personal data is no longer merely an option; it has become an administrative obligation that reflects the requirements of the rule of law and strengthens trust between the government and citizens in the digital environment. We summarize the manifestations of this administrative obligation as follows:

Firstly: The legal obligation to comply with the laws governing data collection and processing.

Secondly: Informing citizens about how their data is collected and the purpose for which it is used.

Thirdly: The administration processes data by collecting, recording, storing, matching, encrypting, deleting, or destroying it. This process is carried out by natural persons, public or private legal entities, or through service providers.

Fourthly: Prior oversight exercised by the National Authority for the Protection of Personal Data: The establishment of the National Authority for the Protection of Personal Data is a concrete implementation of Article 47 of the 2020 Constitution, with the aim of striking a balance between the requirements of public order and security on the one hand, and the rights and freedoms of individuals on the other[12]. It is an independent administrative authority with legal personality and financial and administrative autonomy[13].

Among the functions of the National Authority, as set forth in Article 25 of Law No. 18-07, as amended and supplemented: Article 25 of Law No. 18-07, as amended and supplemented:

1- Granting licenses and receiving authorizations related to the processing of personal data.
2- Informing data subjects and data controllers of their rights and obligations.
3- Providing advice to individuals and entities that process personal data or conduct experiments or activities that by their nature lead to such processing.
4- Receive objections, appeals, and complaints regarding the processing of personal data and inform data subjects of the outcome.
5- Authorize the transfer of personal data abroad in accordance with the specified legal conditions.
6- Order the necessary changes to protect personal data.
7- Ordering the closure, withdrawal, or destruction of data.
8- Publishing the licenses granted and opinions issued in the National Registry for the Protection of Personal Data.
9- Submitting any proposal that would simplify and improve the legislative and regulatory framework for the processing of personal data.
10- Develop cooperative relationships with similar foreign authorities, taking into account the principle of reciprocity.

E.ISSN: 2661-7404 Academic Journal of Legal and Political Researchs P.ISSN:2571-9971
Year: 2026 Vol : 10 No : 02 Page : 243 - 251

11- Imposing administrative sanctions ranging from warnings, reprimands, temporary or permanent revocation of the permit or license, and fines in the event that the data controller violates the procedures established by law[14].

12- Establishing standards in the field of personal data protection.

13- Establishing rules of conduct and ethics governing the processing of personal data.

The legislature has also granted it the authority to carry out a range of measures, such as conducting investigations and inspecting the premises where data is processed; and, in the course of performing its duties[15], the competent public prosecutor shall be notified immediately upon the discovery of facts that may constitute a criminal offense.

An examination of the various powers vested in this authority reveals the extent of its technical and regulatory role, which requires specialized expertise in data processing—particularly since this is explicitly stipulated in the authority's mandate—making it a pivotal and effective mechanism for protecting human rights in the field of data processing and ensuring the security of various information systems to mitigate their negative impacts [16].

Fifthly: Control exercised by the data subject through the provision of consent prior to processing, as stipulated in Article 7 of Law 18-07; conversely, the data subject may withdraw their consent at any time, taking into account that there are cases that do not require the individual's consent, which can be summarized as follows [17]:

1- To perform a contract to which the data subject is a party or to take steps at the data subject's request prior to entering into a contract.

2- To protect the vital interests of the data subject, if the data subject is physically or legally incapable of giving consent.

3- To carry out a task that falls within the scope of public interest or the exercise of public authority by the data controller or a third party to whom the data is disclosed.

Sixthly: Compliance with professional confidentiality and the security of data processing to prevent loss, damage, or unauthorized access.

SECOND REQUIREMENT: CRIMINAL PROTECTION OF PERSONAL DATA

Despite the apparent administrative compliance mentioned above, the administration may fail to comply and thus be subject to penalties, a matter addressed by the legislature in the amended and supplemented Law No. 18-07.

Firstly: Penalties For Processing Data Without the Data Subject's Consent:

The processing of data requires the consent of the data subject, as confirmed by Article 7 of Law No. 18-07, except in cases of necessary processing. The legislature has established a penalty of imprisonment for a term of two to five years and a fine of 100,000 to 500,000 dinars for violations of this provision.

Secondly: Penalties For Processing Data Without Authorization or a License:

The legislature has established penalties for those who violate the procedures set forth in Article 12, as provided for in Article 56 of Law No. 18-07, as amended and supplemented by Law No. 25-11, which states: "Any person who processes personal data or orders the processing of personal data without complying with the conditions set forth in Article 12 of this Law shall be punished by imprisonment for a term of two to five years and a fine of 200,000 to 500,000 dinars".

E.ISSN: 2661-7404 Academic Journal of Legal and Political Researchs P.ISSN:2571-9971
Year: 2026 Vol : 10 No : 02 Page : 243 - 251

It should be noted that the penalty is linked to the act itself—that is, the processing or the order to process— and therefore, modifying the data by inserting new data in place of the previous data without notifying the National Data Protection Authority is also considered conduct punishable under the same framework set forth in Article 56 referred to above; however, the process of deleting data does not fall within the scope of the penalty provided for in Article 56 by application of logic, since deletion is contrary to processing[18].

Thirdly: Penalties for Transferring Data to a Foreign Country:

The legislature has established a penalty of imprisonment for a term of one to five years and a fine of 500,000 to 100,000 dinars against anyone who transfers personal data to a foreign country in violation of the provisions of Article 44 of Law No. 17-07, as amended and supplemented[19].

What we can conclude from the penalties imposed for transferring data to a foreign country is that they represent the most severe penalties among all those provided for in the amended and supplemented text of Law No. 18-07, which underscores the legislature's concern regarding this sensitive issue. This is because personal data transferred to a foreign country may lead to serious consequences for the data subject or for the state as a whole, depending on the importance of the transferred data[20].

Fourthly: Penalty for Breach of Confidentiality:

The data controller is bound by professional secrecy with respect to the information and data to which they have had access[21]. This obligation extends to all persons who have had access to such information, and any breach of this obligation shall result in a fine as provided for in Article 65 of Law No. 18-07, as amended and supplemented, ranging from 200,000 DZD to 500,000 DZD.

Finally, it should be noted that the legislature has required institutions to establish specialized structures to protect systems and data, counter cyberattacks, and secure sensitive information and personal data, pursuant to Presidential Decree No. 26-07 dated January 7, 2026[22].

Conclusion

The protection of personal data has become one of the most important legal and administrative obligations imposed by the modern digital environment, given its direct connection to individuals' fundamental rights and freedoms. With rapid technological advancements, it has become essential to strengthen legislative and regulatory mechanisms to ensure the secure and transparent handling of data, thereby striking a balance between the demands of digitalization and the need to respect privacy.

Therefore, the effectiveness of protection does not depend solely on the existence of legal provisions, but also on their proper enforcement, the promotion of digital awareness, and the fostering of a culture of responsibility among various stakeholders.

Recommendations:

- ✓ Training public officials and staff in the field of cybersecurity.
- ✓ Adopting modern technical measures such as encryption and regular network monitoring.
- ✓ Strengthening national and international cooperation to combat cross-border crimes involving digital data.

E.ISSN: 2661-7404 Academic Journal of Legal and Political Researchs P.ISSN:2571-9971
Year: 2026 Vol : 10 No : 02 Page : 243 - 251

- ✓ Accelerating Algeria's accession to Convention No. 108 on the Protection of Individuals with regard to Automatic Processing of Personal Data, adopted by the Council of Europe in 1981.

Margins:

[1] Presidential Decree No. 20-442 of 30 December 2020, concerning the constitutional amendment, Official Gazette No. 82.
[2] Decree No. 75-58, dated on 26 September 1975, is included in the Civil Code, Official Gazette No. 78, published on 30 September 1975.
[3] Decree No. 66-156, dated on 8 June, 1966, containing the Penal Code (J.R.A. 49), promulgated on 11 June 1966, as amended and supplemented.
[4] Law No. 2000-03, dated August 5, 2000, containing provisions relating to postal services and wired and wireless communications, Decree No. 48, issued on August 6, 2000, (repealed),
[5] Law No. 09-04, dated August 5, 2009, sets forth specific rules for the prevention and combating of crimes related to information and communication technology, as amended by Decree No. 47, issued on August 16, 2009.
[6] Law No. 18-04, dated May 10, 2018, establishes the rules governing mail and electronic communications; Decree No. 27, issued on May 13, 2018.
[7] Law No. 18-07, dated June 10, 2018, concerning the protection of natural persons with regard to personal data, published in the Official Gazette No. 34 dated June 10, 2018. Amended and supplemented by Law No. 25-11 of July 24, 2025, published in the Official Gazette No. 48 of July 24, 2025.
[8] Nouara Hamlil, "Protection of Personal Data in the Context of E-Government," an article published in the Journal of Law and Political Science, Faculty of Law and Political Science, University of Tizi Ouzou, Vol. 15, No. 2, Algeria, 2020, p. 34.
[9] This was done through the enactment of Law No. 78-17 of 6 January 1978, on Information Technology, Data, and Freedoms, which used the term "personal data" and defined it in Article 4 as: "information that, in any form whatsoever, directly or indirectly, allows for the identification of natural persons". However, the French legislature adopted the term "personal data" with the enactment of Law No. 2004-801, which amended and supplemented Law No. 78-17; Article 2 of that law defines personal data as data that enables the identification of a natural person.
[10] Safia Bachtan, Legal Protection of Privacy: A Comparative Study, Ph.D. Thesis, Faculty of Law and Political Science, Mouloud Mammeri University of Tizi Ouzou, Algeria, 2012, p. 233.
[11] Article 303 bis of the Algerian Penal Code: "Any person who intentionally infringes upon the privacy of others, by any means whatsoever, shall be punished by imprisonment for a term of six (6) months to three (3) years and a fine of 50,000 to 300,000 dinars...".
[12] Abdelhadi Ben Zita, "The Need to Establish an Independent Administrative Authority as a Mechanism for the Legal Protection of Personal Data in the Face of the Use of Information Technology," Al-Haqiqa Journal, Ahmed Draia University, Adrar, Vol. 39, 2016, p. 72.
[13] It consists of 16 members appointed by presidential decree for a renewable term of five (5) years. Article 23 of Law No. 18-07 defines the composition of this authority as follows:

Three (03) individuals, including the President, are selected by the President of the Republic from among those with expertise in the National Authority's field of work.
Three (03) judges nominated by the Supreme Judicial Council from among the judges of the Supreme Court and the Council of State.
One member from each chamber of Parliament, selected by the Speaker of each chamber after consultation with the leaders of the parliamentary groups.
One (1) representative from the National Human Rights Council
One (1) representative from the Minister of National Defense

One (1) representative from the Minister of Foreign Affairs
One (1) representative from the Minister in charge of the Interior
One (1) representative from the Minister of Justice and Keeper of the Seals
One (1) representative from the Minister in charge of Postal Services, Telecommunications, Technologies, and Digitalization
One (1) representative from the Minister in charge of Health
One (1) representative from the Minister of Labor, Employment, and Social Security

[14] See Article 46 of Law No. 18-07, as amended and supplemented.
[15] See Article 49 of Law No. 18-07, as amended and supplemented.
[16] Abdelhadi Ben Zita, op. cit., pp. 77, 79.
[17] See Article 7, Paragraph 2 of Law 18-07.
[18] Azzedine Tebache, "Criminal Protection of Personal Data in Algerian Legislation: A Study in Light of Law No. 18-07 on the Protection of Natural Persons with Regard to the Processing of Personal Data," Academic Journal of the Researcher, Vol. 02, 2018, p. 40.
[19] See Article 67 of Law No. 18-07, as amended and supplemented.
[20] Abdelhadi Kahlaoui, Abdelhadi Ben Zita, "Mechanisms for the Protection of Personal Data Under Law No. 18-07 on the Protection of Natural Persons with Regard to the Processing of Personal Data," Journal of Law and Political Science, Vol. 7, No. 2, 2021, p. 125.
[21] See Articles 38 and 39 of Law No. 18-07, as amended and supplemented.
[22] Presidential Decree No. 26-07, dated on 7 January 2026, establishes a structure responsible for information system security and data protection in public institutions, administrations, and agencies, pursuant to Decree No. 04 issued on 18 January 2026.

Bibliography List setting:

Legal Texts

1. Presidential Decree No. 20-442, concerning the constitutional amendment, Official Gazette No. 82, Algeria, 30 December 2020.
2. Ordinance No. 75-58, containing the Civil Code, Official Gazette No. 78, Algeria, 30 September 1975.
3. Ordinance No. 66-156, containing the Penal Code, Official Gazette No. 49, Algeria, 11 June 1966, as amended and supplemented.
4. Law No. 2000-03, concerning postal services and wired and wireless telecommunications, Official Gazette No. 48, Algeria, 6 August 2000 (repealed).
5. Law No. 09-04, laying down specific rules for the prevention and combating of crimes related to information and communication technologies, Official Gazette No. 47, Algeria, 16 August 2009.
6. Law No. 18-04, laying down the rules governing postal services and electronic communications, Official Gazette No. 27, Algeria, 13 May 2018.
7. Law No. 18-07, concerning the protection of natural persons with regard to the processing of personal data, Official Gazette No. 34, Algeria, 10 June 2018, amended and supplemented by Law No. 25-11, Official Gazette No. 48, Algeria, 24 July 2025.
8. Law No. 78-17, relating to Information Technology, Data Files and Civil Liberties, France, 6 January 1978.
9. Law No. 2004-801, amending and supplementing Law No. 78-17 relating to Information Technology, Data Files and Civil Liberties, France, 6 August 2004.

10. Presidential Decree No. 26-07, establishing a structure responsible for information system security and data protection in public institutions, administrations and agencies, Official Gazette No. 04, Algeria, 18 January 2026.

Journal Articles

11. Nouara Hamlil, "Protection of Personal Data in the Context of E-Government," *Journal of Law and Political Science*, Faculty of Law and Political Science, University of Tizi Ouzou, Vol. 15, No. 2, Algeria, 2020, p. 34.

12. Abdelhadi Ben Zita, "The Need to Establish an Independent Administrative Authority as a Mechanism for the Legal Protection of Personal Data in the Face of the Use of Information Technology," *Al-Haqiqa Journal*, Ahmed Draia University, Adrar, Vol. 39, 2016, p. 72.

13. Azzedine Tebache, "Criminal Protection of Personal Data in Algerian Legislation: A Study in Light of Law No. 18-07 on the Protection of Natural Persons with Regard to the Processing of Personal Data," *Academic Journal of the Researcher*, Vol. 02, 2018, p. 40.

14. Abdelhadi Kahlaoui, Abdelhadi Ben Zita, "Mechanisms for the Protection of Personal Data Under Law No. 18-07 on the Protection of Natural Persons with Regard to the Processing of Personal Data," *Journal of Law and Political Science*, Vol. 7, No. 2, 2021, p. 125.

Theses / Dissertations

15. Safia Bachtan, *Legal Protection of Privacy: A Comparative Study*, Ph.D. Thesis, Faculty of Law and Political Science, Mouloud Mammeri University of Tizi Ouzou, Algeria, 2012, p. 233.