Journal of Ecohumanism
2025
Volume: 4, No: 4, pp. 2062 – 2072
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i4.6955

The Legal Protection of the Right to Digital Privacy in Algeria

Hanane Guedda[1], Fadhila Chabane[2]

Abstract

This paper addresses the legal protection of the right to digital privacy in Algeria. This topic holds great importance due to the growing challenges and threats faced by this right in the digital sphere. In response, the Algerian legislator has established a constitutional and legal framework to ensure its effective protection amid the rapidly evolving technological revolution. The Constitution first guarantees citizens the right to privacy, followed by the right to the confidentiality of their communications and correspondence in all forms. To implement these protections, the legislator enacted Law No. 18-07 on the protection of natural persons in the processing of personal data, and created an independent authority responsible for safeguarding individuals' rights, freedoms, and private lives from the risks posed by information and communication technologies.

Keywords: *Right to privacy – Digital space – Personal data – Data processing – Information and communication technology – Cybercrime.*

Received: 25/02/2025 **Accepted**: 24/04/2025 **Published:** 15/05/2025

Introduction

The right to privacy is a fundamental human right. In the modern era, a new dimension of privacy has emerged — digital privacy, which is linked to the online sphere where sensitive personal data and information are exchanged. With the massive expansion of information technology use in Algeria, including digital commerce and electronic public services, risks of privacy violations have increased significantly. These include identity theft, unauthorized surveillance, and unlicensed data exploitation.

Thus, ensuring legal protection for the right to privacy has become an essential condition for building trust in electronic interactions and for guaranteeing that citizens can exercise their individual freedoms without fear of their personal information being violated. Although the Algerian Constitution guarantees the right to privacy in all its forms, and various legal texts address cybersecurity, the challenge lies in the adequacy and effectiveness of these provisions in confronting the growing complexity of digital threats.

The importance of this subject stems from the significance of digital privacy as a human right, closely linked to human dignity and individual freedom. This has become especially relevant with the increasing collection and processing of personal data by government institutions and private companies, raising serious concerns about potential violations of the right to privacy. Individuals routinely share their personal information online, exposing themselves to risks of data theft, espionage, or misuse of data for commercial or other purposes. Therefore, the legal protection of personal data and the confidentiality of electronic communications has become a fundamental requirement for establishing digital trust and protecting individual freedoms.

The objective of this study is to analyze and evaluate the constitutional and legislative framework governing the protection of the right to digital privacy in Algeria. It seeks to assess the adequacy and effectiveness of existing legal texts — such as the Constitution, the Penal Code, and special data protection laws — in addressing modern cyber threats. Hence, the central research question arises:

[1] Faculty of Law and Political Science, University of El Oued, guedda-hanane@univ-eloued.dz
[2] Faculty of Law and Political Science, University of El Oued, chabane-fadhila@univ-eloued.dz

Journal of Ecohumanism
2025
Volume: 4, No: 4, pp. 2062 – 2072
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i4.6955

How have the Algerian constitutional and legislative frameworks organized the legal protection of the right to digital privacy?

To answer this question, the study adopts a descriptive methodology, by presenting relevant legal provisions and describing the current state of privacy protection in Algeria. It also employs an analytical approach to interpret constitutional articles recognizing this right, analyze provisions of Law No. 18-07 on personal data processing, and review relevant articles of the Algerian Penal Code, which criminalize violations of privacy in all its forms.

To comprehensively address the topic, the study is divided into two main sections:

- The first section examines the constitutional framework guaranteeing the right to privacy, highlighting the constitutional value of the right to private life and the constitutional safeguards for digital privacy.

- The second section explores the legislative framework that operationalizes this protection, focusing on laws that safeguard natural persons in personal data processing and criminalize acts that violate the right to privacy in all its dimensions.

First: The Constitutional Framework for Ensuring the Right to Privacy

The Constitution serves as the primary guarantor of individual rights and freedoms. The right to privacy is one of the inherent human rights that has received both international and domestic protection, as enshrined in constitutional documents. In this section, we will explain the constitutional value of the right to private life and the constitutional guarantees of the right to digital privacy.

The Constitutional Value of the Right to Private Life

The right to private life is linked to several definitions that relate to the essence of human existence and individuality — the right of every person to live a life that suits them, provided it does not violate public order. These rights are categorized under fundamental headings such as the right to privacy and the right to the confidentiality of correspondence, which all reflect the individual's right to privacy as a personal right that must be safeguarded, with legal penalties imposed for any violation.

The right to privacy is considered one of the first-generation rights and freedoms, recognized by international conventions and treaties as one of the most essential human rights. The Universal Declaration of Human Rights (1948) was the first to enshrine this right. Article 12 stipulates that:

"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[i]."

Similarly, the International Covenant on Civil and Political Rights (1966) reaffirmed this right in Article 17, which provides that:

"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[ii]."

This international recognition of the right to privacy, and its connection to human existence and daily life, placed it at the forefront of rights acknowledged by national constitutions, including the Algerian Constitution. Through its various provisions, the Algerian Constitution established principles protecting privacy in all its forms, which have been consistently reaffirmed across successive constitutional texts, from the 1963 Constitution to the most recent 2020 amendment.

Journal of Ecohumanism
2025
Volume: 4, No: 4, pp. 2062 – 2072
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i4.6955

The 1963 Constitution, in its second chapter titled *"Fundamental Rights"*, included several personal rights such as the inviolability of the home and the confidentiality of correspondence[iii]. The 1976 Constitution similarly enshrined these protections in Chapter IV of Title I, under *"Fundamental Freedoms and the Rights of Man and Citizen."* It affirmed the protection of personal rights, beginning with the right to security, followed by the right to privacy, stipulating that no one may be subjected to interference in their private life or honour, and that the law shall ensure their protection. It also guaranteed the confidentiality of correspondence and private communications in all forms, as well as the inviolability of the home[iv].

Given the importance of the right to privacy as a personal right intrinsically linked to human existence and dignity, it was preserved in the 1989 constitutional amendment, despite the political and economic changes introduced by that revision[v]. The 1996 amendment also maintained the same approach as its predecessor, reaffirming legal protection for the inviolability of citizens' private lives, their honour, and the confidentiality of their correspondence[vi].

These constitutional provisions establish protection for the right to private life. As is clear from the constitutional text, this right encompasses several dimensions: an individual's personal integrity, honour, home, and personal correspondence — all of which are considered inviolable. This recognition grants individuals the right to maintain the confidentiality of matters arising from their private lives.

The right to private life has two fundamental dimensions:

- The first is the freedom to conduct one's private life without interference.
- The second is the right to protect the privacy resulting from the exercise of that life — meaning every individual has the right to preserve the confidentiality of their communications and correspondence, and to prevent the publication of any information related to their private life without their consent[vii].

The constitutional recognition of the inviolability of citizens' private lives and honour has granted this right protection by the Constitutional Judge. The Algerian Constitutional Council derived from the constitutional provisions recognizing this right the principle of the inviolability of private life, in the course of its review of the constitutionality of the Organic Law on Elections.

In one of its opinions, the Council stated:

"Considering that the legislator's objective, when allowing certain individuals to obtain a copy of the municipal electoral list, was to ensure the rights of parties participating in elections; and considering that the exercise of this right cannot occur without respecting the rights of others as recognized by the Constitution, particularly Article 63 thereof; and considering that Articles 35 and 39(1) of the Constitution establish the principle of the inviolability of citizens' private lives and provide for their protection by law; thus, any violation of the rights enshrined in this principle shall be punishable by law[viii]."

This demonstrates that the Algerian Constitutional Council granted the principle of the inviolability of private life a legal value equivalent to that of constitutional provisions themselves.

From the above, it becomes evident that the constitutional judiciary — represented formerly by the Constitutional Council and currently by the Constitutional Court — plays a vital and effective role in protecting the rights and freedoms recognized by the Constitution. This is achieved through constitutional review of laws and regulations, including those concerning privacy. Such judicial oversight constitutes a decisive check on both the legislative and executive branches, thereby ensuring the protection of individual privacy rights.

Journal of Ecohumanism
2025
Volume: 4, No: 4, pp. 2062 – 2072
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i4.6955

The Constitutional Guarantee of the Right to Digital Privacy

The right to privacy is one of the personal rights that the Constitution has granted special attention to. The private life of citizens, as well as their honour and correspondence in all forms, are inviolable, and no interference with them is permitted without a reasoned order issued by the judicial authority.

The Constitution emphasizes that any restriction on these rights must be within the framework of the law and based on a judicially justified decision, as judicial oversight constitutes the essential foundation for ensuring protection against arbitrary limitations of privacy.

However, the remarkable advances in information and communication technologies have significantly impacted individuals' privacy and have led to a reconsideration of the general concept of the inviolability of private life as a constitutional principle. This development is reflected in Article 47 (paragraph 2) of the 2020 Constitutional Amendment, which guarantees the inviolability of private correspondence and communications in all forms.

This protection does not apply solely to traditional forms of correspondence and communication but extends the concept of privacy to include digital correspondence and communications, such as email and social media exchanges. Any interference with these rights must be justified by a judicial order.

The digital era has greatly contributed to the erosion of users' privacy, as the constant recording, storage, and sharing of information and data across online platforms have made personal data — once private — easily accessible to everyone.

The right to privacy also encompasses the inviolability of the home, as the Constitution guarantees that the State shall ensure the protection of homes from violation. Searches may only be conducted in accordance with the law, with respect for the sanctity of the home, and under a written order issued by a competent judicial authority[ix].

This constitutional provision ensures that the home remains a private sanctuary protected from arbitrary searches or intrusive actions by state authorities, and it establishes a fundamental limitation on state intervention, stipulating that searches may occur only upon judicial authorization to prevent abuse of power.

Moreover, personal data have been recognized as an integral component of digital privacy. The final paragraph of Article 47 of the 2020 Constitution explicitly states:

"The protection of natural persons in the processing of personal data is a fundamental right guaranteed by law, and its violation shall be punishable."

This article serves as a strong constitutional foundation for ensuring the protection of personal data. In implementation, the legislator intervened in 2018 by enacting Law No. 18-07, concerning the protection of natural persons in the processing of personal data. This law established the National Authority for the Protection of Personal Data, tasked with safeguarding individuals' private lives in cooperation with the judicial authorities.

In the same context, Article 55 of the 2020 Constitutional Amendment recognizes citizens' right to access information, documents, and statistics, as well as to obtain and share them, provided that the exercise of this right does not infringe upon the private lives or rights of others, the legitimate interests of institutions, or the requirements of national security.

To further reinforce the sanctity of private life, Article 81 of the 2020 Constitution stipulates:

Journal of Ecohumanism
2025
Volume: 4, No: 4, pp. 2062 – 2072
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i4.6955

"Every person shall exercise all freedoms in a manner that respects the rights of others as recognized by the Constitution, particularly respect for the right to honour and private life, and the protection of the family, childhood, and youth."

These two articles establish a constitutional principle affirming that while individuals may exercise the rights and freedoms recognized by the Constitution, such exercise is subject to the essential condition of not violating citizens' privacy in any of its dimensions, and of maintaining full respect for it.

Although the Constitution provides a robust framework for privacy protection, its practical implementation faces several challenges, notably the need to balance individual rights of certain groups with the general right to privacy guaranteed to all citizens, as well as to reconcile personal freedoms with the requirements of public order.

Secondly: The Legislative Framework for Ensuring the Right to Digital Privacy

The protection of personal data constitutes the core of safeguarding an individual's right to digital privacy. Therefore, many national legislations have hastened to enact laws that protect individuals in the context of processing personal data. In this regard, the Algerian legislator issued Law No. 18-07 on the protection of natural persons in the processing of personal data. In addition, the Penal Code had already criminalized acts that infringe upon privacy. The following section explains these mechanisms in detail.

Protection of Personal Data

Law No. 18-07, concerning the protection of natural persons in the processing of personal data, guarantees the protection of individuals' private lives and dignity in the digital age by imposing strict rules on institutions that collect and process such data.
This law also established the National Authority for the Protection of Personal Data, which serves as a supervisory body responsible for ensuring that personal data processing complies with the provisions of the law. The following sections clarify the substance of this law and the supervisory role of this authority.

The Personal Data Protection Law

Law No. 18-07 is considered the cornerstone in protecting the fundamental rights and freedoms of natural persons, particularly their right to privacy in relation to personal data processing.
Its objective is to achieve a balance between the requirements of developing the digital economy and the necessity of protecting individuals' privacy.

The Algerian legislator provided clear definitions of the terminology related to the processing of personal data to avoid ambiguity or multiple interpretations that might lead to the loss of rights or the commission of violations in their name.

Personal data is defined as:

"Any information, regardless of its medium, relating to an identified or identifiable person — referred to hereinafter as the data subject — directly or indirectly, particularly by reference to an identification number or to one or more elements specific to their physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity[x]."

Accordingly, personal data can be divided into two main categories[xi]:

1. Direct personal data, such as name, surname, date of birth, postal and email address, genetic and health data, personal photographs, civil status, personal background, place of residence, place of work, etc.

Journal of Ecohumanism
2025
Volume: 4, No: 4, pp. 2062 – 2072
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i4.6955

2. Indirect personal data, such as phone numbers, social security numbers, national identification numbers, passwords, biological and biometric data, bank account numbers, fingerprints, DNA profiles, and any other information connected to a person, whether directly or indirectly.

Processing refers to any operation or set of operations performed on personal data, whether by automated or non-automated means, such as collection, recording, or organization. Processing of personal data may only be carried out with the explicit consent of the data subject or their legal representative, authorizing the processing of their personal data by manual or electronic means. This consent may be withdrawn at any time[xii].

Furthermore, the law obliges any entity collecting and using data to comply with a set of principles, including legality, fairness, and transparency, by clearly informing the data subject of the identity of the data controller and the purpose of processing[xiii].

It also requires that data be collected for specific, clear, and legitimate purposes, and prohibits further processing incompatible with those purposes[xiv].

The legislator prohibits retaining personal data longer than necessary to achieve the purposes for which it was collected and processed. The data controller is required to maintain the confidentiality of data and to take all appropriate technical and organizational measures to ensure its security and protection from damage, loss, or unauthorized access[xv].

Data subjects are granted several rights to enable them to protect their personal data, the most important of which is the right to information.The law requires the data controller to inform every person whose personal data is being collected of the controller's identity (or their representative), the purpose of processing, and any other useful information — even if the data is collected indirectly and without direct contact[xvi].

When information is collected through open networks, the person concerned must be informed — unless they are already aware — that their personal data may circulate in these networks without safety guarantees and may be subject to unauthorized reading or use by third parties[xvii].

The data subject also has the right to obtain confirmation of whether their data is being processed, the purposes and categories of processing, and to receive, in an understandable format, the personal data being processed.
They have the right to access this data and to request its correction, updating, or completion if it is incomplete or inaccurate. Moreover, they have the right to object, for legitimate reasons, to the processing of their personal data — particularly if it is used for marketing or advertising purposes by the data controller[xviii].

Conversely, the data controller is obliged to take all necessary technical and preventive measures to protect personal data from hacking, damage, or unlawful use, especially when transmitted through a network. These measures must increase in rigor depending on the sensitivity and value of the data concerned[xix].

In addition, electronic certification service providers must process personal data solely for issuing and maintaining certificates linked to electronic signatures for the concerned individuals and are prohibited from using such data for any other purpose unless with the explicit consent of the data subjects. Likewise, electronic communication service providers are required — after adopting all necessary data protection guarantees — to notify both the National Authority and the data subject in case of any breach affecting their privacy[xx].

The National Authority for the Protection of Personal Data

To ensure the implementation of the provisions of Law No. 18-07 on the protection of natural persons in the processing of personal data, the National Authority for the Protection of Personal Data was established.

Journal of Ecohumanism
2025
Volume: 4, No: 4, pp. 2062 – 2072
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i4.6955

It is an independent administrative authority created under the supervision of the President of the Republic, endowed with legal personality and financial and administrative autonomy. Its mission is to protect the rights, freedoms, and private lives of individuals from the risks posed by information and communication technologies.

The law entrusted this authority with supervisory and sanctioning functions aimed at preventing violations of the right to privacy. The following sections detail these roles.

Supervisory Functions of the National Authority for the Protection of Personal Data

According to Article 25 of Law No. 18-07, the legislator defined the supervisory responsibilities of the Authority, which include:

- Granting licenses and receiving declarations related to the processing of personal data.
- Receiving appeals and complaints regarding the implementation of personal data processing and informing the concerned parties of the outcomes.

The Authority's preventive measures may take place before data processing begins, by deciding to subject a proposed data processing operation to a prior authorization regime if, upon reviewing the declaration, it determines that the intended processing presents clear risks to the protection of private life, freedoms, or fundamental rights of individuals[xxi].

The licenses issued by the Authority and the declarations submitted to it are recorded and published in the National Register for the Protection of Personal Data. This register must include the identity of the data controller, enabling data subjects to exercise their rights under the law[xxii].

After data processing has begun, the Authority also provides advice and consultations to individuals or entities engaged in processing personal data, or to those conducting experiments or research that may involve such processing.

In exercising its supervisory powers, the Authority may immediately inform the competent Public Prosecutor if it observes facts that may constitute a criminal offense.

Sanctioning (Enforcement) Functions of the National Authority for the Protection of Personal Data

According to Article 46 of Law No. 18-07, in cases of violation of the provisions of the law, the National Authority for the Protection of Personal Data may take the following administrative measures:

- Warning: A formal notice issued by the Authority to inform the data controller of the legal consequences of violating the law's provisions.
- Formal Notice: A legal notification granting the data controller a specific time period to comply with their obligations before further legal action is taken.
- Temporary or Permanent Withdrawal: Suspension (for up to one year) or permanent withdrawal of the declaration receipt or processing authorization.
- Fine: A financial penalty payable to the state treasury, which may reach 500,000 Algerian Dinars, imposed on any data controller who, without legitimate reason, refuses to grant the rights of information, access, objection, or correction as stipulated in the law.

Decisions issued by the Authority are subject to judicial review before the Administrative Courts. The data controller affected by any of the aforementioned administrative measures may appeal to the Council of State (Conseil d'État) in accordance with the applicable legislation.

Journal of Ecohumanism
2025
Volume: 4, No: 4, pp. 2062 – 2072
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i4.6955

Under Article 49 of Law No. 18-07, when investigating violations affecting privacy through the processing of personal data, the National Authority may conduct investigations and inspections of premises where data processing occurs.
It has the right to access processed data and all related information and documents, regardless of their medium, and professional secrecy may not be invoked to obstruct its work.

Furthermore, the aforementioned law includes criminal penalties for violators of its provisions.

Criminal Protection of Digital Privacy

The criminal legislator has intervened to criminalize acts that violate privacy in the digital age, particularly through the prohibition of illegal interception and unauthorized access to information systems.

The crime of illegal interception is punishable under Article 303 bis of the Algerian Penal Code, which provides for imprisonment from six months to three years and a fine ranging from 50,000 to 300,000 Algerian dinars for anyone who violates the sanctity of private life or discloses secrets.
The article specifies that such violations include recording, capturing, transmitting, or using images or private or confidential conversations without the consent of the person concerned[xxiii].

Furthermore, Article 303 bis 1 imposes the same penalties on anyone who possesses, distributes, makes accessible to the public or third parties, or uses in any way recordings, images, or documents obtained through the acts described in Article 303 bis. Attempting to commit these offenses is punishable by the same penalties as those applied to the completed crimes.

This article explicitly refers to cybercrimes, criminalizing the publication or use of private photos, recordings, or documents by any means — including online defamation and the misuse of social media platforms.

The legislator also criminalized unauthorized access to information systems, a cybercrime that poses a major threat to cybersecurity, involving unauthorized entry into or interference with information systems to steal data or disrupt operations[xxiv].

According to Article 394 bis of the Penal Code,

"Anyone who fraudulently enters or remains in all or part of an automated data processing system, or attempts to do so, shall be punished by imprisonment from three (3) months to one (1) year and a fine of 50,000 to 100,000 Algerian dinars."

This article addresses illegal hacking of automated data processing systems and punishes the mere act of entry or unauthorized presence, even without damage. The penalty is increased when such access results in deletion, alteration, or destruction of data, or renders the system inoperative.
Its objective is to combat the growing wave of cybercrimes by criminalizing attacks on automated data systems, including data erasure, modification, or sabotage[xxv].

Additional legislation has contributed to data protection and cybercrime prevention, including:

- Law No. 09-04 (2009) on the Prevention of Crimes Related to Information and Communication Technologies, which defines ICT-related offenses as:

"Crimes involving automated data processing systems as defined in the Penal Code, or any crime committed or facilitated through an information system or an electronic communication network[xxvi]."

- Law No. 15-04 (2015) on the General Rules of Electronic Signature and Certification, which establishes a legal framework for electronic signatures and digital certificates, aiming to enhance trust and security in electronic transactions and promote e-commerce[xxvii].

Journal of Ecohumanism
2025
Volume: 4, No: 4, pp. 2062 – 2072
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i4.6955

Conclusion

From the above, it becomes evident that the Algerian Constitution provides a comprehensive and robust framework for protecting the right to privacy.Through specific provisions safeguarding private life, correspondence, and the inviolability of the home, the Constitution ensures a solid legal shield for individuals.
Despite the challenges of enforcement, the emphasis on judicial oversight and the requirement for justification of any legal restriction are essential pillars of privacy protection.

This constitutional foundation serves as the cornerstone for future legal developments aimed at strengthening citizens' privacy in an increasingly interconnected world.

Main Findings

1. International recognition of the right to privacy as an inherent human right, regardless of nationality.

2. Constitutional recognition of privacy rights, including in Algeria, where several principles safeguard this right, although implementation challenges persist.

3. The constitutional framework provides strong protection for all aspects of privacy, including digital privacy.

4. The legislator introduced specific legal measures to criminalize any violation of digital privacy in any form.

5. Law No. 18-07 enforces strict rules on institutions handling personal data, protecting individuals' private lives and dignity in the digital era.

6. The creation of the National Authority for the Protection of Personal Data aims to safeguard the rights, freedoms, and private lives of individuals against ICT-related risks.

Recommendations

- Periodic review of laws and regulations to keep pace with rapid technological evolution and the emergence of new digital threats.

- Strengthening the role of the National Authority for the Protection of Personal Data to ensure effective enforcement.

- Raising legal awareness among individuals, companies, and system administrators about the risks of data breaches.

- Promoting international cooperation to combat cybercrime and enhance data protection.

- Addressing implementation challenges, especially those related to cross-border cybercrimes.

---

[i] Universal Declaration of Human Rights, adopted by the United Nations General Assembly under Resolution No. 217 on December 10, 1948, to which Algeria acceded pursuant to Article 11 of the Constitution of the People's Democratic Republic of Algeria of 1963.

Available at the following link:

Journal of Ecohumanism
2025
Volume: 4, No: 4, pp. 2062 – 2072
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i4.6955

https://www.un.org/ar/universal-declaration-human-rights-

[ii] Presidential Decree No. 89-67, dated May 16, 1989, concerning Algeria's accession to the International Covenant on Civil and Political Rights and the Optional Protocol to the International Covenant on Civil and Political Rights, approved by the United Nations General Assembly on December 16, 1966. Official Gazette of the People's Democratic Republic of Algeria, No. 20, issued on May 17, 1989. The content of these instruments was published as an annex in Official Gazette No. 11, issued on February 26, 1997, p. 33.

[iii] Article 14 of the 1963 Constitution, dated September 10, 1963, Official Gazette of the People's Democratic Republic of Algeria, No. 64 of 1963.

Available on the website of the Office of the Prime Minister at:

http://www.premier-ministre.gov.dz/ar/documents/textes-de-references.html

[iv] Articles 49 and 50 of Ordinance No. 76-97, dated November 23, 1976, promulgating the Constitution of the People's Democratic Republic of Algeria. Official Gazette, No. 94, issued on November 24, 1976, p. 1302.

[v] Articles 37 and 38 of Presidential Decree No. 89-18, dated February 28, 1989, concerning the publication of the text of the constitutional amendment approved by referendum on February 23, 1989. Official Gazette, No. 9, issued on March 1, 1989, p. 293.

[vi] rticles 39 and 40 of Presidential Decree No. 96-438, dated December 7, 1996, promulgating the text of the constitutional amendment approved by referendum on November 28, 1996. Official Gazette, No. 76, issued on December 8, 1996, p. 12.

[vii] Ahmed Fathi Sorour, Constitutional Protection of Rights and Freedoms, 2nd Edition, Dar Al-Shorouk, Cairo (Egypt), 2000, p. 732.

[viii] Opinion No. 01/R.QA/MD/04, dated February 5, 2004, concerning the constitutional conformity of the organic law amending and supplementing Ordinance No. 97-07 of March 6, 1997, relating to the electoral system. Official Gazette, No. 09, issued on February 11, 2004, p. 17.

[ix] See Article 48 of Presidential Decree No. 20-442, dated December 30, 2020, promulgating the constitutional amendment approved by referendum on November 1, 2020. Official Gazette, No. 82, issued on December 30, 2020, p. 13.

[x] See Article 3 of Law No. 18-07, dated June 10, 2018, relating to the protection of natural persons in the processing of personal data. Official Gazette, No. 34, issued on June 10, 2018, p. 12.

[xi] Meriem Loukal, "International and National Legal Protection of Personal Data in Digital Space," Journal of Legal and Political Sciences, Vol. 10, No. 1, 2019, p. 1309.

[xii] Article 7 of Law No. 18-07, dated June 10, 2018, on the protection of natural persons in the field of personal data processing, previously cited, p. 13.

[xiii] The data controller, according to Article 3 of Law No. 18-07, is defined as:

"Any natural or legal person, public or private, or any other entity that determines, alone or jointly with others, the purposes and means of processing personal data."

[xiv] Article 9 of Law No. 18-07, dated June 10, 2018, previously cited, p. 14.

[xv] Same article, same page.

[xvi] Mohamed El-'Aidani and Youssef Rezoug, "Protection of Personal Data in Algeria in Light of Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data," Ma'alem Journal of Legal and Political Studies, University Center of Tindouf, Issue No. 5, December 2018, p. 124.

[xvii] See Article 32 of Law No. 18-07, previously cited, p. 19.

[xviii] See Articles 35 and 36 of the same law, p. 19.

[xix] El-'Aidani and Rezoug, previously cited, p. 126.

[xx] See Articles 42 and 43 of Law No. 18-07, previously cited, p. 20.

[xxi] For more information about prior authorization, see:

Adel Qarrana and Fares Bouhidid, "Functions of the National Authority for the Protection of Personal Data in Algerian Legislation," Journal of Legal and Social Sciences, Ziane Achour University – Djelfa, Vol. 6, No. 2, June 2021, p. 1063 ff.

[xxii] See Articles 25 and 28 of Law No. 18-07, previously cited, pp. 17–18.

[xxiii] See Article 303 bis of Law No. 06-23, dated December 20, 2006, amending and supplementing Ordinance No. 66-156 of June 8, 1966, containing the Penal Code. Official Gazette, No. 84, issued on December 23, 2006, p. 23.

[xxiv] Najat Abbaoui, "Legislative Differences in Criminalizing Unauthorized Access to Information Systems," Journal of Law and Political Sciences, University Center of Salhi Ahmed – Naama, Issue No. 1, January 2016, p. 157.

Journal of Ecohumanism
2025
Volume: 4, No: 4, pp. 2062 – 2072
ISSN: 2752-6798 (Print) | ISSN 2752-6801 (Online)
https://ecohumanism.co.uk/joe/ecohumanism
DOI: https://doi.org/10.62754/joe.v4i4.6955

[xxv] See Article 394 bis of Law No. 04-15, dated November 10, 2004, amending and supplementing Ordinance No. 66-156 of June 8, 1966, containing the Penal Code. Official Gazette, No. 71, issued on November 10, 2004, p. 12.

[xxvi] Article 2 of Law No. 09-04, dated August 5, 2009, containing specific provisions on the prevention and combating of crimes related to information and communication technologies. Official Gazette, No. 47, issued on August 6, 2009, p. 5.

[xxvii] Law No. 15-14, dated February 1, 2015, determining the general rules relating to electronic certification and electronic signatures. Official Gazette, No. 06, issued on February 6, 2015, p. 6.