SEPTEMBER 2025 (№35)
Volume 11; Issue 3; Page No. 32-41
ISSN: 2346-7916 (Print)
ISSN: 2587-5043 (Online)

INTERNATIONAL JOURNAL OF LAW: "LAW AND WORLD" www.lawandworld.ge

https://doi.org/10.36475/11.3.3

Securing Electronic Data and Safeguarding Personal Privacy in the Digital Environment *(Pursuant to the Provisions of Algerian Law No. 18-07 on the Protection of Personal Data)*

Fadhel Aicha
PhD in Law, contract professor, lawyer, University of Sfax, Tunisia
misaichamsdk12@gmail.com

ARTICLE INFO

Article History:

Received	22.05.2025
Accepted	21.07.2025
Published	30.09.2025

Keywords:

Data, Privacy, Personal information, Security, Digital age, Protection of personal data

ABSTRACT

In the context of rapid digital advancement, securing data has become a central concern for both individuals and institutions. Data security refers to a broad set of technical and organizational practices aimed at preventing unauthorized access, alteration, or destruction of information. Rather than relying solely on encryption or access control tools, effective data protection involves a multilayered approach that includes user awareness, preventive policy frameworks, and continuous monitoring.

Modern challenges to data security are increasingly complex due to the exponential growth of digital information and the evolving nature of cyber threats. Attackers now exploit vulnerabilities using sophisticated techniques, often bypassing traditional defenses. This highlights the urgent need for proactive strategies that combine technological safeguards with human-centered practices such as employee training and ethical data handling.

Furthermore, the legal dimension of data security has gained prominence, with many jurisdictions enforcing stricter regulations to protect individuals' rights. Legal compliance—particularly with frameworks like the General Data Protection Regulation (GDPR)—is no longer optional but essential for

maintaining organizational credibility and avoiding penalties.

Ultimately, securing data in today's interconnected world requires an ongoing commitment. It is not a fixed goal but a dynamic process that evolves with technological, legal, and social developments. Ensuring data security strengthens public trust, reinforces privacy principles, and lays a solid foundation for sustainable digital transformation.

INTRODUCTION

Data and information constitute one of the most critical pillars of any company, often regarded as its most valuable assets. In the event of a breach, a company is bound to incur substantial losses, with its reputation inevitably damaged. Failure to address such breaches and their consequences effectively could result in the leakage of client data and information, ultimately leading to the company's collapse. Therefore, protecting the IT infrastructure that houses this data becomes imperative.

With the global escalation of cyber-attacks, the demand for security products and services has risen significantly, driven by persistent threats and the evolving nature of cyber-attack patterns.

Data security encompasses the protective strategies implemented to shield data from unauthorized access, ensuring the confidentiality, integrity, and availability of databases. Optimal methodologies in data security include techniques such as data encryption, key management, data masking, data subsetting, and data redaction, alongside controls for privileged user access, auditing, and monitoring.

Data, being a vital asset of any firm, must be safeguarded against unwanted access. Data breaches, unsuccessful audits, and non-adherence to regulatory mandates can lead to reputational harm, forfeiture of corporate ownership rights, compromised intellectual property, and penalties for regulatory non-compliance.

Under the General Data Protection Regulation (GDPR) of the European Union, data breaches may incur fines of up to 4% of an organization's global annual turnover, frequently resulting in significant financial losses. Financial information, medical records, intellectual property, and personally identifiable information (PII) are all considered sensitive data. Safeguarding this data is crucial to avert breaches and maintain regulatory compliance.

Databases function as essential storage of sensitive information, rendering them a primary target for data thieves. Data intruders are often classified into two categories: external users and internal users.

External users include various entities, such as individual hackers and cybercriminals, that seek to disrupt business operations or attain financial profit. They encompass organized crime syndicates and state-sponsored organizations aiming to perpetrate fraud or instigate disruptions on a national or global level.

Internal users may encompass current or former workers, inquisitive persons, clients, or partners who misuse their position of trust to appropriate data or whose mistakes accidentally result in security breaches. Both external and internal users present threats to the security of personal data, financial information, trade secrets, and regulated data.

The safeguarding of personal data has become increasingly crucial in the contemporary digital age. Due to swift technological improvements and the pervasive usage of the internet, individuals frequently disclose their personal information online. Personal data is collected,

kept, and utilized by multiple entities across social media platforms and e-commerce websites, frequently without explicit consent or awareness. This engenders significant privacy issues and underscores the necessity for robust safeguards to protect personal information.

In the contemporary digital era, data functions as the essential resource for enterprises, governments, and individuals. Data, encompassing sensitive consumer information and intellectual property, constitutes the foundation upon which institutions function and make pivotal decisions. Nonetheless, due to the increasing dependence on technology and a continuously changing threat environment, the significance of data security is paramount. It is no longer solely about safeguarding sensitive information; it has become a strategic necessity that can influence an organization's reputation, financial viability, and potentially its survival.

To address the increasing risks to the privacy and confidentiality of personal data in the digital realm, a number of international organizations have put forward and implemented policies. The Organization for Economic Co-operation and Development (OECD) has underlined the necessity of bolstering the right to privacy in order to facilitate the unrestricted flow of personal data. Similarly, the UN General Assembly established rules for the control of personal data files in its Resolution 45/95.

The European Union established regulations to safeguard individuals against the processing of digital data. Numerous countries have also enacted legal provisions to safeguard personal data. Algeria, like other nations, has prioritized the establishment of a legal framework to protect individuals' personal data.

STUDY PROBLEM

This study seeks to analyze the procedures and techniques for safeguarding personal data under Algerian law by evaluating the principal aspects and clauses of Law No. 07/18, enacted on June 10, 2018, about safeguarding people when processing their personal information.

This leads us to the following key question: **How has the Algerian legislator secured digital data to protect individuals' personal privacy?**

We have structured this article as follows:

- The conceptual framework for personal data;
- The legal framework of the National Authority for the Protection of Personal Data;
- Procedures for processing personal data.

METHODOLOGY

The research employs a doctrinal legal methodology, centered on the analysis of primary and secondary legal sources, including the Algerian Constitution, Law No. 18-07 on the protection of personal data, and related legislative acts. This approach is complemented by the examination of international instruments such as the GDPR, OECD guidelines, and UN resolutions, which provide a comparative framework for situating Algerian law within broader international standards. The study also incorporates a critical interpretative dimension by evaluating the institutional independence and effectiveness of the National Authority for the Protection of Personal Data. This combined approach ensures both descriptive and analytical insights, allowing the research to highlight legal strengths while identifying potential gaps in implementation.

1. THE CONCEPTUAL FRAMEWORK FOR PERSONAL DATA

1.1 Definition of personal data

Maintaining a person's right to privacy depends critically on the protection of their personal information. National legislatures have therefore quickly passed legislation to protect individuals while collecting personal data. The Algerian lawmaker who passed Law No. 18-07 on June 10, 2018, regarding the protection of natural

persons in the use of personal data is one example. This law established the "National Authority for the Protection of Personal Data", a crucial organization to protect the handling of personal data while respecting people's right to privacy.

Any information, regardless of type, that directly or indirectly relates to an identifiable individual is referred to as personal data. An identifying number or other components of a person's physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity can be used as the primary means of identification.

Based on this definition, personal data is categorized into two main types:

- Direct Personal Data: This includes data of an explicit personal nature, such as names, surnames, postal and email addresses, genetic data, health records, criminal records, personal photographs, civil status, résumés, birth dates, places of residence, and workplaces;
- Indirectly identifiable information includes things like phone numbers, social security numbers, national identity card numbers, passwords, bank account numbers, fingerprints, genetic profiles, and biological and biometric data.

1.2 Enshrining the protection of personal data in Algerian law

In compliance with Article 46 of the 2016 amended Algerian Constitution, the National Authority for the Protection of Personal Data was established by the Algerian parliament. This was aimed at striking a balance between the requirements of public security on the one hand and the rights and freedoms of individuals on the other.[1] This principle was reaffirmed in Article 47 of the 2020 Algerian Constitution.[2]

The National Authority is an independent administrative body in charge of safeguarding personal information. It operates without administrative or hierarchical oversight and has legal individuality as well as financial and administrative autonomy.[3] The President of the Republic appoints the "National Authority", an independent administrative body for the protection of personal data, as specified in Article 22 of Law No. 18-07. The Authority, which has its headquarters in Algiers, is financially and administratively independent in addition to having legal individuality. The budget is subject to the relevant financial control regulations and is part of the state budget.

In the framework of processing personal data, the law created a number of measures to protect persons. The establishment of the National Authority for the Protection of Personal Data is among the most crucial mechanisms. The Authority is designated as an autonomous administrative entity, possessing legal identity, as well as financial and administrative autonomy.

This study's significance pertains to the regulations governing the Authority's autonomy, which constitute a key feature distinguishing it from other traditional administrative bodies in the state. However, despite the formal aspects of independence reflected in various provisions, this independence is, in practice, relative and closer to a theoretical ideal than a tangible reality.

1 Official Gazette of the People's Democratic Republic of Algeria. (2016, March 7). Issue No. 14. "The law protects the inviolability of a citizen's private life and honor, which cannot be compromised. All private communications and correspondence are guaranteed to remain confidential. Only a well-reasoned order from the legal authority may violate these rights in any manner. Violations of this provision are punishable by law. A fundamental right protected by law is the protection of natural persons in the processing of personal data; infractions of this right can result in legal repercussions".

2 Official Gazette of the People's Democratic Republic of Algeria. (2020, December 30). Issue No. 82. "Every person is entitled to the protection of their personal honor and private life. Regardless of the format, everyone has the right to keep their private communications and correspondence private. Only a well-reasoned order from the judicial authority may violate the rights outlined in the first and second paragraphs. One fundamental right is the protection of individuals when personal data is processed. The law punishes any infringement of these rights".

3 Ghazal, N. (2019). The protection of natural persons in the field of personal data. Algerian Journal of Legal and Political Sciences, p. 125.

2. THE LEGISLATIVE FRAMEWORK FOR THE NATIONAL AUTHORITY FOR THE PROTECTION OF PERSONAL DATA

2.1 The legal framework for the protection of personal data

A successful legislative framework for personal data protection necessitates the presence of procedures and resources for proper implementation and oversight to ensure the correct application of the law. Personal data protection cannot be achieved without establishing an administrative body responsible for enforcing the rules and provisions of the law.

Article 23 of Law No. 18-07 stipulates the formation of this administrative body, consisting of 16 members, appointed by presidential decree. While the president is responsible for appointing the chairperson of the authority, the members are selected by their peers from within the councils to which they belong. The composition is as follows:

Six advisors, including:

- Two current or former members of the Council of State, with a rank no less than that of an advisor;
- Two current or former members of the Court of Cassation, with a rank no less than that of an advisor;
- Two current or former members of the Court of Auditors, with a rank no less than that of an advisor;
- The general assembly of each distinct institution elects these members.

2.2 Composition of the National Authority for the Protection of Personal Data

Regarding the nomination process for each member, the Algerian legislator specifies that the composition of the Authority includes:

- The President of the Republic nominated three people, including the president, from among specialists in the operations of the National Authority;
- The High Judicial Council selected three Supreme Court and Council of State judges.[4]

The Authority is also empowered to seek assistance from any qualified individual for consultation and support in carrying out its duties. Additionally, it includes an executive secretariat and personnel employed to assist the executive body in fulfilling its responsibilities.[5]

Referring to the composition of the National Authority, the Algerian legislator required that the Authority be supported by specialists. While the legislation allows for external consultation, it would have been preferable to explicitly include university professors and researchers specializing in rights, freedoms, and information technology. Their expertise, particularly in comparative legislation and studies conducted in this field, could greatly enhance the Authority's effectiveness.

The Algerian legislator specified the appointment of three experts in the Authority's field of work, reflecting the multidisciplinary nature of its jurisdiction, which encompasses judicial, quasi-judicial, and administrative domains. Notably, in some legislations, bodies tasked with protecting personal data are granted extensive regulatory and executive powers, including criminal penalties for non-compliance with the Authority's orders.[6,7]

Under the Algerian legal system, the President of the Republic is given the power to choose the Authority's president. This central-

4 Ordinary Law No. 18-07. (2018, June 10). Concerning the protection of natural persons in the processing of personal data. Official Gazette of the People's Democratic Republic of Algeria, No. 34, Art. 23(3).

5 Ordinary Law No. 18-07. (2018, June 10). Concerning the protection of natural persons in the processing of personal data. Official Gazette of the People's Democratic Republic of Algeria, No. 34, Art. 23.

6 This is consistent with the approach taken by the British legislator in Law No. 98 on the Protection of Personal Data in the digital environment, which established a personal data protection authority known as the Office of the Information Commissioner.

7 Khalawi, A., Ben Zitah, A. (2022). The independent administrative authority for the Protection of Personal Data: A study in French and Algerian law. Algerian Journal of Legal and Political Sciences, p. 125.

ization of appointment authority risks undermining the independence of the Authority in implementing its decisions. The legislator limited the President's role to appointing, renewing membership, and terminating appointments through a presidential decree, requiring the Authority to submit an annual report to the Republic's President.[8]

The Authority is tasked with issuing opinions on the data processing activities referenced in Articles 31 and 32 of Law No. 18-07. Additionally, it develops and publishes guidelines, recommendations, and standards to facilitate compliance with personal data protection regulations. It is also responsible for conducting preliminary risk assessments related to data processing activities by data controllers and their contractors.

It is primarily an ethical rather than a legal requirement for members of the National Authority for the Protection of Personal Data to take an oath. This reinforces their commitment to exercising their legal powers with impartiality, objectivity, and integrity, particularly regarding confidential information. Such an approach ensures that all members of the Authority remain independent and are not subject to any oversight or external control.

Before beginning their duties, members of the National Authority are sworn in at the Algiers Court of Justice.[9] However, it is noteworthy that the process of election is absent in determining membership within the Authority. The Algerian legislator established a five-year term for membership, subject to renewal,[10] comprising people chosen for their legal or technical proficiency in personal data protection.[11]

The concept of competence underpins membership in the National Authority for the Protection of Personal Data.[12]

3. PROCEDURES FOR PROCESSING PERSONAL DATA

3. 1 Processing of personal data

All grievances and inquiries submitted by data subjects, organizations, associations, or entities are addressed through the examination and verification of the complaint's subject matter. The complainant is informed of the investigation's progress and results within a designated timeframe. The Authority addresses requests for opinions from public bodies and courts as needed and offers consultations to persons and organizations engaged in or intending to engage in automated personal data processing.

In accordance with Article 40 of the Code of Illegal Procedure, the Authority promptly informs the Public Prosecutor of any illegal activities or violations. Moreover, under Article 19 of Law No. 87-17, the Authority may issue a special decision assigning one or more of its members or the Secretary-General to carry out investigations or delegate its agents and departments to conduct verification procedures. When required, it may also obtain copies of all relevant documents and informational materials necessary for its mission.

The Authority may create a list of data processing operations that are anticipated to pose major risks, which must undergo prior consultation as mandated by Article 90 of Law No. 87-17. Furthermore, Article 25, paragraph 1, of Law No. 18-07 mandates that the National Authority for the Protection of Personal Data ensure compli-

8 Bala, A. (2021). The national authority for the protection of personal data: Between independence and subordination. Algerian Journal of Human Security, p. 783.

9 Before assuming their duties, members of the National Authority take an oath before the Court of Algiers in the following form: "I swear by Almighty God to perform my duties as a member of the National Authority for the Protection of Personal Data with full independence, impartiality, honor, and integrity, and to maintain the confidentiality of deliberations".

10 Ordinary Law No. 18-07. (2018, June 10). Concerning the protection of natural persons in the processing of personal data. Official Gazette of the People's Democratic Republic of Algeria, No. 34, Art. 23(4).

11 Ordinary Law No. 18-07. (2018, June 10). Concerning the protection of natural persons in the processing of personal data. Official Gazette of the People's Democratic Republic of Algeria, No. 34, Art. 23 (2).

12 Wataba, K. (2019). The legal nature of independent administrative authorities in Algeria and comparative systems. Journal of Legal and Political Sciences, April, p. 7.

ance with the legislation pertaining to personal data processing as specified in Law No. 18-07. It also ensures that the utilization of information and communication technology does not jeopardize individual rights, public liberties, or personal privacy.

The Authority may offer recommendations and adopt individual or regulatory decisions as mandated by law in the execution of its responsibilities. Furthermore, the Authority presents an annual public report to the President of the Republic and the Prime Minister, outlining the fulfillment of its purpose.

3.2 Role of the data controller

The National Authority for the Protection of Personal Data and the data controller must collaborate. The Authority's operations are considered to be hampered by any interference with its operations, such as preventing on-site investigations, denying its members or agents access to necessary documents, giving information that conflicts with records that were already in existence at the time of the request, or failing to provide clear and straightforward information. Additionally, submitting incomplete or intentionally erroneous documents to obscure the truth constitutes an offense punishable under Article 61 of Law No. 18-07.

Furthermore, the Authority's operations are governed by a set of regulations. The president of the National Authority must respond expeditiously and guarantee the confidentiality of personal data accessible in the course of their responsibilities, even after their term ends. The president and members of the Authority are prohibited from holding any interests in organizations that operate within the domain of personal data processing.

The Authority is responsible for the construction and maintenance of a National Register for the Protection of Personal Data. This register contains all statements made to the National Authority, authorizations granted, regulatory texts pertaining to public records, and other pertinent information. The register is accessible to individuals in accordance with legal and regulatory procedures.

The National Authority for the Protection of Personal Data is authorized by Law No. 18-07 to allow data controllers to transfer personal data to other countries, provided that the Authority determines that the recipient country offers a sufficient degree of protection for people's privacy, fundamental freedoms, and rights, along with appropriate security measures. Additionally, the Authority must confirm that neither public safety nor the state's fundamental interests are jeopardized by the transfer.

But there are exceptions to every rule. In certain circumstances, data controllers may transmit personal data to a nation that does not fit the above-listed requirements, including:

- The specific agreement of the person in question;
- Situations in which the transfer is essential to safeguard an individual's life or uphold the public interest;
- The execution or conclusion of contracts;
- The execution of initiatives pertaining to international judicial collaboration;
- Identifying, diagnosing, or treating illnesses;
- Adherence to bilateral or multilateral agreements in which Algeria has participated.[13]

Law No. 18-07 offers essential safeguards for national data that was once available to foreign entities operating in Algeria, including telecommunications firms, internet service providers, and embassies managing several visa applications daily. Without laws that forbid such actions, these apps frequently include private information that may be readily exported to other nations.[14]

Monitoring the post-processing operations is

13 Ashkar-Jabbour, M., Jabbour, M. (2018). Personal data and Arab laws: Security concerns and individual rights. Arab Center for Legal and Judicial Research, p. 81.

14 Ordinary Law No. 18-07. (2018, June 10). Concerning the protection of natural persons in the processing of personal data. Official Gazette of the People's Democratic Republic of Algeria, No. 34, Art. 44.

one of the responsibilities given to the National Authority. The National Authority is tasked with a number of duties under Article 25 of Law No. 18-07, including consulting with people and organizations that process personal data or carrying out research or trials that could result in such processing. It also manages complaints, appeals, and objections pertaining to the processing of personal data, making sure that people are aware of the results.[15]

The Authority instructs persons and data controllers regarding their rights and responsibilities. This includes the right to be informed in advance of the data controller's identity and the reason for processing. Additionally, it guarantees that all pertinent information is conveyed, including the data's recipient, the requirement to reply, the repercussions of non-compliance, and concerns about data transfers to foreign nations.

In cases where information is used in an open network, individuals must be informed that their data may circulate in such networks without safety guarantees and could be subject to unauthorized access and use by third parties.[16]

Ordering the required modifications to safeguard personal data and mandating the closure, withdrawal, or destruction of poorly processed personal data are among the Authority's other responsibilities.[17]

The Algerian legislator sought to provide criminal protection for personal data under the Electronic Commerce Law No. 18-05 through the regulation of "direct prospecting" as defined in Law No. 18-07.[18] This practice involves accessing personal data without the prior consent of the individual concerned, typically for purposes such as research, inspection, or prospecting for potential customers. This is achieved by compiling informational files containing personal data, including names, addresses, phone numbers, and consumption patterns or customer opinions obtained through electronic communications. Such data is used to categorize customers and generate targeted commercial offers specific to each category.[19]

The Electronic Commerce Law empowers customers to manage their personal data by requiring prior notification before data processing, enabling them to consent to or decline such processing. Law No. 18-07 establishes an exception to the prerequisite of prior consent when processing is essential to fulfill a legitimate interest of the data controller or recipient, contingent upon the respect for the interests, rights, and fundamental freedoms of the individual involved.[20]

Under these conditions, the right to object functions as a protective measure for consumers, balancing the individual's right to privacy with the legitimate interests of the data controller.

Regarding electronic certification, the Algerian legislator, under Law No. 15-04, regulated the activities of service providers by establishing authorities such as the National Authority for Electronic Certification, the Governmental Authority for Electronic Certification, and the Economic Authority for Electronic Certification. Articles 20(2)[21] and 27[22] of the Electronic Certification Law

15 Ordinary Law No. 18-07. (2018, June 10). Concerning the protection of natural persons in the processing of personal data. Official Gazette of the People's Democratic Republic of Algeria, No. 34, Art. 25.

16 Aidani, M., Rizk, Y. (2018). The Protection of Personal Data in Algeria in light of Law No. 18-07. Ma'alam Journal of Legal and Political Studies, 5, p. 127.

17 Ordinary Law No. 18-07. (2018, June 10). Concerning the protection of natural persons in the processing of personal data (as amended and supplemented). Official Gazette of the People's Democratic Republic of Algeria, No. 34, Art. 28

18 Ibid., Article 3 defines "direct prospecting" as: "The sending of any message, regardless of its medium or nature, aimed at the direct or indirect promotion of goods or services or the reputation of a person who sells goods or provides services".

19 Khalil, W. (2016). The role of direct marketing in achieving customer loyalty (Master's thesis, Ferhat Abbas University, Setif, Faculty of Economic, Commercial, and Management Sciences). p. 8.

20 Ordinary Law No. 18-07. (2018, June 10). Concerning the protection of natural persons in the processing of personal data (as amended and supplemented). *Official Gazette of the People's Democratic Republic of Algeria*, No. 34, Art. 7 (final paragraph).

21 Ordinary Law No. 15-04. (2015, February 1). Establishing general rules regarding electronic signatures and certification. Official Gazette of the People's Democratic Republic of Algeria, Art. 20(2).

22 The nature, composition, organization, and functioning of this governmental authority for electronic certi-

delegate the organization of the governmental and economic authorities to executive decrees.

CONCLUSION

In conclusion, securing digital data and safeguarding the privacy of personal information requires establishing boundaries that subject violators to criminal liability. This protection, while relative, necessitates heightened awareness and vigilance from individuals, particularly regarding these boundaries, to avoid infringing on others' privacy. Legislators in Tunisia and Algeria have both sought to protect the private lives of natural and legal persons in a restricted but consistent manner. The establishment of organizations devoted to protecting personal data—which is directly related to individual privacy—has reflected this protection.

Through the establishment of the National Authority for the Protection of Personal Data pursuant to Law No. 18-07, the Algerian legislators have formalized this protection, which gives the Authority certain responsibilities. These efforts are particularly significant in light of the rapid technological advancements and the proliferation of information technology. The Authority supports data controllers by helping them comply with the law and assists data subjects in exercising their rights as prescribed by legal provisions.

The National Authority's role in personal data processing highlights the importance of ensuring data security, which can be summarized as follows:

- Privacy Protection: Information security safeguards individuals' and organizations' data against unauthorized access, thereby preserving their privacy;
- Reputation Preservation: Failure to protect information can result in significant losses for companies and organizations, as well as damage to their reputation;
- Legal Compliance: Numerous regulations and laws mandate organizations to protect sensitive information and adhere to security requirements;
- Countering Cyber Threats: In a world facing escalating cyber threats, information security is essential for combating these risks and ensuring system stability.

fication shall be determined through regulation.

Key Findings:

- Data security is a dynamic and multifaceted challenge in our digital age. Organizations and individuals must invest in robust security measures and treat threats with seriousness. By educating users, employing advanced technologies, and complying with legal requirements, we can safeguard our information and ensure the sustainability of a progressive digital world;
- In response to technological problems, the Algerian legislator established the National Authority for the Protection of Personal Data to ensure the protection of personal information;
- Law No. 18-07 strengthens Algeria's legislative framework to protect freedoms and rights. It mandates the prior and explicit consent of the data subject before processing their data, even if the processing is authorized. The right to revoke consent is always available to the data subject. This legal framework aims to curb the prevailing chaos in the field, particularly as individuals routinely provide their data to public entities, private organizations, telecommunications companies, or foreign embassies in Algeria without knowing its ultimate fate;
- A National Authority, known as the "National Authority", was also established under the law, and its main responsibility is to supervise its enforcement. The Authority is responsible for granting permits and licenses to entities wishing to process personal data, conducting investigations, and imposing sanctions on violators of the law.

REFERENCES

Scientific literature:

Aidani, M. Rizk, Y. (2018). The protection of personal data in Algeria in light of Law No. 18-07. Ma'alam Journal of Legal and Political Studies, 5.

Ashkar-Jabbour, M., Jabbour, M. (2018). Personal data and Arab laws: Security concerns and individual rights. Arab Center for Legal and Judicial Research.

Bala, A. (2021). The national authority for the protection of personal data: Between independence and subordination. Algerian Journal of Human Security.

Ghazal, N. (2019). The protection of natural persons in the field of personal data. Algerian Journal of Legal and Political Sciences.

Khalawi, A., Ben Zitah, A. (2022). The independent administrative authority for the protection of personal data: A study in French and Algerian law. Algerian Journal of Legal and Political Sciences.

Khalil, W. (2016). The role of direct marketing in achieving customer loyalty (Master's thesis in Commercial Sciences, Specialization in Marketing Studies and Research, Faculty of Economic, Commercial, and Management Sciences, Ferhat Abbas University, Setif).

Wataba, K. (2019). The legal nature of independent administrative authorities in Algeria and comparative systems. Journal of Legal and Political Sciences, April.

Legal Acts/Official Documents:

Official Gazette of the People's Democratic Republic of Algeria. (2016, March 7). Issue No. 14.

Official Gazette of the People's Democratic Republic of Algeria. (2020, December 30). Issue No. 82.

Ordinary Law No. 15-04. (2015, February 1). Establishing general rules regarding electronic signatures and certification. Official Gazette of the People's Democratic Republic of Algeria, Art. 20(2).

Ordinary Law No. 18-07. (2018, June 10). Concerning the protection of natural persons in the processing of personal data. Official Gazette of the People's Democratic Republic of Algeria, No. 34, Art. 23(3).