

RESEARCH ARTICLE	Protection of Personal Data in Cyberspace in Light of Algerian Legislation	
Elbordj Khadidja	Doctor	
	University of Ghardaia	
	Algeria	
	Email: elbordj.khadidja@univ-ghardaia.edu.dz	
Doi Serial	https://doi.org/10.56334/sei/8.6.67	
Keywords	Protection, Personal data, Cyberspace, Cybercrime.	
Abstract		
<p>The field of information systems and technology has witnessed tremendous development over the past few decades across various domains, becoming an essential part of individuals' daily lives and significantly influencing how they interact with the world around them. This field has encompassed many social groups, each according to its specific needs and requirements, potentially offering benefits as well as posing challenges alike. Cyberspace in Algeria, as in other countries, is considered a double-edged sword for individuals: it carries significant benefits while simultaneously opening the door to risks that threaten the privacy and security of individuals through the harmful exploitation of their personal data and unauthorized use. Accordingly, the Algerian legislator has moved to regulate this area through legislation dedicated to the protection of personal data.</p>		
Citation		
Elbordj Kh. (2025). Protection of Personal Data in Cyberspace in Light of Algerian Legislation. <i>Science, Education and Innovations in the Context of Modern Problems</i> , 8(6), 615-621; doi:10.56352/sei/8.6.67. https://imcra-az.org/archive/364-science-education-and-innovations-in-the-context-of-modern-problems-issue-6-volvihi-2025.html		
Licensed		
© 2025 The Author(s). Published by Science, Education and Innovations in the context of modern problems (SEI) by IMCRA - International Meetings and Journals Research Association (Azerbaijan). This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/). PACS: 61.46.		
Science, Education and Innovations in the Context of Modern Problems, Issue 6, Vol.VIII, 2025		
Received: 10.02.2025	Accepted: 16.04.2025	Published: 29.05.2025 (available online)

Introduction:

Our present era is known as the age of technological revolution and knowledge explosion. The last decade has witnessed tremendous development in the field of information technology, which forms the foundation of cyberspace—a space that includes all networks, systems, and devices connected to the Internet. It represents the digital infrastructure that today constitutes an indispensable environment, becoming an urgent necessity for most of the world's population. However, one of the worst byproducts of this technological progress is the targeting and illicit exploitation of individuals' personal data.

Hence, the issue of protecting personal data has become a vital concern in the age of

technology. The protection of individuals' private lives has always been, and continues to be, one of the primary goals that laws aim to achieve. This has prompted legislators to develop deterrent legal provisions to ensure the protection of personal data and to establish advanced technical strategies and mechanisms to guarantee the security of personally identifiable information.

Based on the above, this topic is considered of great importance in the digital age in which we live today, where we have witnessed numerous instances of personal data being targeted and exploited. This raises questions regarding the stance of the Algerian legislator on the issue of personal data protection. Thus, the central research problem can be formulated as follows: Has the Algerian legislator ensured the necessary

protection for personal data in cyberspace?

The nature of this topic necessitates reliance on the analytical method by analyzing the legal texts regulating the issue of personal data protection and drawing conclusions. The aim is to evaluate the effectiveness of the existing legislation.

Additionally, the comparative method has been used by comparing Algerian legislative texts with those of other countries, in order to identify the strengths and weaknesses of Algerian law and to attempt to address its shortcomings.

The nature of the research problem requires addressing the topic through two main sections: first, the conceptual framework that connects personal data to cyberspace; and second, the guarantees that ensure the protection of personal data.

Our current era is known as the age of technological revolution and knowledge explosion. The last decade has witnessed tremendous progress in the field of information technology, which forms the foundation of cyberspace. Cyberspace encompasses all networks, systems, and devices connected to the Internet. It is a digital infrastructure that has today become an indispensable environment, a vital necessity for most people around the world. However, one of the worst by-products of this technological advancement is the targeting and unlawful exploitation of individuals' personal data.

Hence, the issue of personal data protection is of vital importance in the age of technology. The protection of individuals' privacy has always been one of the objectives pursued by legal systems. This has prompted legislators to establish strict legal provisions to enshrine the protection of personal data and to develop advanced technical strategies and tools to ensure this protection.

Based on the above, this topic is considered of great importance in the digital age in which we live. We have witnessed numerous cases of personal data being targeted and misused, prompting questions about the stance of the Algerian legislator regarding the protection of personal data. Therefore, the central research question of this study is as follows:

Has the Algerian legislator ensured adequate protection for personal data in cyberspace?

The nature of this topic requires reliance on

the analytical method, by analyzing the legal texts that regulate personal data protection, drawing conclusions, and understanding the intended objectives. In addition, the comparative method was also consulted, through a comparison between Algerian legal texts and those of other legislations to highlight the strengths and weaknesses of Algerian law in an effort to address its shortcomings.

The nature of the issue requires examining the topic through two main axes: First, we will address the Conceptual Framework to link personal data and cyberspace.

Second, we will address the Legal Mechanisms for the Protection of Personal Data in Cyberspace.

Part One: The Conceptual Framework of Personal Data and Cyberspace

Technology has provided immense opportunities for learning and knowledge development through information and communication technologies. It has also facilitated many services and tasks by saving time and effort. Moreover, it has allowed for the exchange of information, ideas, cultures, and interaction between people who share similar interests and tendencies. These are social entities composed of individuals or institutions connected by ties that result from their mutual interactions.¹

However, some users of this digital environment have exploited this space and violated individuals' privacy. In response, many countries and parties have sought to implement a range of legal measures to ensure the right to privacy, particularly in the increasingly technologically developed digital environment.

Algeria has also enacted a law to protect natural persons in the field of processing personal data, as stated in Law No. 18/07, which we will address alongside the concept of cyberspace.

1. The Concept of Personal Data

This technological revolution has enabled access to individuals' personal data and has exposed it to circulation and dissemination.

¹ Ramadan Ben Khamma, *Children and Social Media Networks: Challenges, Risks, and Mechanisms of Protection and Guidance - A Theoretical Approach*, *Al-Mi'yar Journal*, No. 03, University of Tissemsilt, Algeria, 2022, p. 644.

Through personal data, one can identify an individual directly or indirectly. Therefore, we will address the definition of personal data and then determine its types.

a. The Emergence of Personal Data Protection

Personal data refers to information that can be used to identify a person; thus, this data must be protected—especially with the integration of technology into modern life, which has increased the potential for the collection, processing, and transfer of personal data. As a result, laws emerged to regulate data protection in the digital environment, first at the national level and later internationally, eventually evolving into an independent legal branch.²

The first law related to data protection appeared in the German state of Hesse in 1970 and in Sweden in 1973. This was followed by the OECD Guidelines in 1980, which were later revised in 2013.³ Similarly, the UN issued its 1990 guidelines on regulating the use of computerized personal data files.⁴

Laws on personal data protection have since been adopted by many countries, including Algeria in 2018, which issued specific legislation to protect natural persons in the processing of personal data, with a national authority responsible for enforcing the law.

b. Definition of Personal Data

Regarding the definition of personal data, we will focus on what is stated in Law No. 18/07 on the protection of natural persons in the processing of personal data. Article 3 defines personal data as: “Any information, regardless of its medium, related to an identified or identifiable person, hereinafter referred to as ‘the data subject,’ either directly or indirectly, in particular by reference to an identification number or to one or more ele-

ments specific to their physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity.”

From this definition, it is clear that the legislator broadly encompassed all types of personal data and listed them as examples. Any of the data mentioned in the definition may be considered personal data that must be protected, whether processed manually or electronically, as long as it concerns the data subject.⁵

For the purposes of this law, the “data subject” refers exclusively to natural persons, meaning that legal persons are excluded from this protection.

2. The Concept of Cyberspace

Cyberspace is considered a virtual environment formed by a network of digital systems, including digital devices and software that interact and exchange information. This allows for the performance of various activities related to our daily lives. Therefore, it is crucial to understand the historical background and definition of the term.

a. Historical Origins of Cyberspace

The term “cyberspace” was first used in 1982 by William Gibson. It is a combination of two words: “cybernetics,” which means the science of automatic control, and “space.” Thus, the term “cyberspace” was coined.⁶

Science fiction writer William Gibson described the term as a strange concept: “A collective hallucination experienced daily by billions of legitimate operators in every nation... A graphic representation of data abstracted from the banks of every computer in the human system”.⁷

Definition of Cyberspace :

The French National Cybersecurity Agency (ANSSI – *Agence Nationale de Sécurité des Systèmes d'Information*) defines cyberspace

² Sheikh Al-Hussein Mohammed Yahya and Sayed Mohammed Sayed Ahmed, *The Legal Protection of Personal Data (A Comparative Study of British and Emirati Law)*, *Journal of Judiciary and Law*, Judicial Department, No. 04, Abu Dhabi, 2018, p. 41.

³ Organization for Economic Co-operation and Development (OECD), *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (2013) [C(80)58/FINAL, as amended on 11 July 2013 by C(2013)79].

⁴ United Nations, Economic and Social Council, Human Rights Committee, *Guidelines for the Regulation of Computerized Personal Data Files*, 20 February 1990.

⁵ N. Neiri, “Access to Administrative Documents in Tunisia”, in *Democracy and Administration*, Proceedings of the Conference held in Tunis on 10-11 October 2011, Faculty of Law and Political Science of Tunis, Latrach Editions, Tunis, 2014, p. 131.

⁶ Belafred Latti Lamine and Amhend Barkaouk, *Cyberspace: Actors and Threats*, *Afaq Journal of Sciences*, No. 03, University of Ziane Achour, Djelfa, Algeria, 2024, p. 622.

⁷ Alaa Eddine Farhat, *Cyberspace: Shaping the Battlefield of the 21st Century*, *Journal of Legal and Political Sciences*, No. 03, University of Algiers 1, Algeria, 2019, p. 90.

as:

“A space for communication resulting from the automated interconnection of digital data processing equipment”.⁸

There are also definitions by experts in the field. French expert Bertrand Boyer defines it as:

“A communication space resulting from the global interconnection of digital data processing equipment”.⁹

According to Boyer, cyberspace is a global domain composed of an interconnected network of IT infrastructure, including the Internet, telecommunications networks, computer systems, operational systems, and control mechanisms. It includes both transmitted digital information and service delivery systems beyond the Internet.¹⁰

In contrast to the technical definition, cyberspace is also described as a new homeland—one that belongs neither to geography nor history. It is a land without borders, without memory, and without heritage. It is a space built by electronic information and communication networks. The term *cybernetic space* is linked to cybernetics, the science that studies the flow and control of information in living beings, machines, and social-economic systems.¹¹

Accordingly, we can say that cyberspace is a multifaceted domain that includes the Internet, networks, and digital systems used for communication, information exchange, and task execution, while also offering improved and simplified services. However, on the other hand, it creates significant challenges related to security and privacy that must be recognized and addressed.

Second: Legal Mechanisms for the Protection of Personal Data in Cyberspace

Given the widespread and increasing use of cyberspace, we must be alert to the risks associated with violations of personal privacy. For this purpose, **Law No. 18/07** was

enacted to define the rules for protecting natural persons in the field of processing personal data. It stipulates a set of deterrent penalties for any data controller who violates the provisions of this law. We will address these legal mechanisms as follows:

1. Fundamental Principles for the Protection of Personal Data

Law No. 18/07 establishes a set of principles and obligations that must be respected when collecting, processing, and storing individuals' data. These are internationally recognized standards in this field, and we address them as follows:

a. Prior Consent and Nature of the Data

According to Article 07 of **Law No. 18/07**, the Algerian legislator requires the explicit consent of the data subject for the processing of their personal data. If the data subject lacks full or partial legal capacity, consent is governed by the rules set out in general law.

The legislator also permits the data subject to withdraw their consent regarding the disclosure of their processed personal data to third parties. However, exceptions to this rule were noted, where consent is not required if processing is necessary for the following (as stated in the same article):

- To comply with a legal obligation imposed on the data subject or the data controller;
- To protect the life of the data subject;
- To safeguard the vital interests of the data subject when they are physically or legally unable to express their consent;
- To carry out a task in the public interest or in the exercise of official authority vested in the data controller or in the recipient of the data;
- To achieve a legitimate interest pursued by the data controller or recipient, provided that the fundamental rights and freedoms of the data subject are respected.

In this regard, it would have been preferable if the legislator had provided more detailed definitions of these cases where personal data can be processed without the subject's consent, particularly in the first point, where specifying the identity and affiliation of the data controller would have strengthened

⁸ Sheikh Al-Hussein Mohammed Yahya and Sayed Mohammed Sayed Ahmed, *The Legal Protection of Personal Data (A Comparative Study of British and Emirati Law)*, ibid., p. 42.

⁹ Bertrand Boyer, *Cyberstrategie: Conduire la guerre numérique*, Paris: NUNIS, 2014, p. 25.

¹⁰ Bertrand Boyer, *Cyberstrategie: L'art de la guerre numérique*, Paris: NUNIS, 2012, p. 54.

¹¹ Alaa Eddine Farhat, *Cyberspace: Shaping the Battlefield of the 21st Century*, ibid., p. 90.

ened safeguards.

As for the method of processing, Article 09 of Law No. 18/07 requires that data processing be lawful and fair, for a specific and non-excessive purpose. Data must also be accurate, complete, and updated when necessary and stored in a way that allows identification of natural persons for no longer than the period required for processing.

Regarding the nature of the data, Article 10 of Law No. 18/07 stipulates that data related to crimes, penalties, and security measures may only be processed by the judiciary, public authorities, public service legal entities, and judicial auxiliaries within the scope of their legal authority.

b. Pre-processing Procedures

According to Article 12 of **Law No. 18/07**, unless another legal provision dictates otherwise, all personal data processing operations must either be declared in advance to the national authority or be subject to prior authorization, in accordance with the provisions of this law.

- **Declaration:** A prior declaration, including a commitment to carry out the processing, must be submitted to the national authority. It may be submitted electronically, and a receipt is issued within a maximum of 48 hours. Upon receipt of the declaration, and under their own responsibility, the data controller may commence processing operations.¹² The law also requires that the declaration contain several pieces of information, such as the name and address of the data controller, the nature of the data, and whether the data will be transferred abroad, among other elements.¹³

- **Authorization:** The national authority may subject a specific data processing operation to prior authorization through a reasoned decision if it deems, based on the declaration submitted, that the intended processing presents evident risks to privacy and data protection. The data controller must be notified of this decision within ten days from the date of the declaration.

Under no circumstances may sensitive data

¹² Article 13 of Law No. 18/07 dated June 10, 2018, concerning the protection of natural persons with regard to the processing of personal data, *Official Gazette*, No. 34, issued on June 10, 2018, p. 14.

¹³ Article 14 of the same source.

be processed except where it serves the public interest and is necessary for the fulfillment of legal or regulatory functions by the data controller or with the consent of the data subject, as stipulated in Article 18 of the same law. This article also lists exhaustively the cases in which authorization to process sensitive data may be granted.

Article 20 of the same law specifies the information that must be included in the authorization, which mirrors the contents of the declaration. The decision regarding authorization must be issued within two months from the date of notification, and this period may be extended once by the same duration by a reasoned decision of the authority's president.

2. The National Authority for the Protection of Personal Data

In many countries, independent bodies are established under data protection laws to monitor compliance, ensure responsible handling of personal data by individuals and companies, and uphold privacy standards.

Similarly, Algeria has established a national authority for the protection of personal data, which issues rulings and performs other functions, as detailed below:

a. Legal Framework of the Data Protection Authority

This authority is an independent administrative body with legal personality and financial and administrative autonomy. It is established under the authority of the President of the Republic. Its budget is included in the state budget and is subject to financial oversight according to applicable legislation.¹⁴

The authority is composed of:

- Three experts in the authority's field of work, one of whom serves as president and is appointed by the President of the Republic;
- Three judges proposed by the Supreme Judicial Council from the Supreme Court and the Council of State;
- One member from each chamber of parliament, chosen by the president of each chamber in consultation with the heads of

¹⁴ Article 22 of Law No. 18/07 concerning the protection of natural persons with regard to the processing of personal data.

parliamentary groups;

- Eight representatives from the following entities: the National Human Rights Council, Ministry of National Defense, Ministry of the Interior, Ministry of Justice, Ministry of Post and Telecommunications and Digitalization, Ministry of Health, and Ministry of Labor, Employment, and Social Security.¹⁵

Regarding this composition, it would have been preferable if the legislator had mandated that most members be elected from among judges and technical experts in relevant ministries and independent bodies, with the possibility of consulting other representatives as needed for the authority's functions.

Returning to the National Authority for the Protection of Personal Data, its responsibilities are defined in Article 25 of the same law, including issuing authorizations and receiving declarations related to data processing, informing data subjects and data controllers of their rights and obligations, and providing guidance to individuals and entities involved in or experimenting with data processing activities. The law outlines additional duties as well.

b. Administrative and Penal Sanctions of the National Authority

The national authority may impose administrative sanctions on data controllers who violate the provisions of this law, ranging from warnings to fines of up to 500,000 DZD. Depending on the case, the authority may also, without delay, withdraw a declaration receipt or authorization if it determines that the processing threatens national security or violates public morals or order.¹⁶

Furthermore, Law No. 18/07 includes penal provisions for violations of its provisions. These sanctions range from imprisonment of six months to five years, depending on the nature of the offense, in addition to monetary fines of up to 500,000 DZD.¹⁷

Conclusion

Cyberspace has become an indispensable necessity in our daily lives due to its multi-

faceted uses across all fields. Accordingly, the protection of personal data has become an urgent priority, requiring the adoption of appropriate measures to secure systems, networks, and data through effective cybersecurity. In addition, the establishment of legal and regulatory frameworks is essential to ensure the protection of personal data in this space.

Algeria, like other countries concerned with the protection of personal data in all its forms, including automated processing, has enacted Law No. 18/07 on the protection of natural persons with regard to the processing of personal data. The effectiveness of this authority in safeguarding personal data requires a range of efforts and measures, including:

- The legislator should provide greater detail regarding the circumstances under which personal data may be processed without the data subject's consent, to guarantee the protection of their rights and fundamental freedoms.
- It would be preferable if the legislator, in determining the composition of the National Authority for the Protection of Personal Data, relied on judges and technical experts, while also engaging advisors as stipulated in the law.
- The national authority should conclude agreements and cooperate with countries that are more advanced in this field, in order to benefit from their experience—especially given the increasing use of cyberspace and the corresponding rise in the risk of cybercrimes.

¹⁵ Article 23 of the same source.

¹⁶ Articles 46 and following of Law No. 18/07 concerning the protection of natural persons with regard to the processing of personal data.

¹⁷ Article 54 and following of the same source.

References

1. Article 13 of Law No. 18/07 dated June 10, 2018, concerning the protection of natural persons with regard to the processing of personal data, *Official Gazette*, No. 34, issued on June 10, 2018, p. 14.
2. Sheikh Al-Hussein Mohammed Yahya and Sayed Mohammed Sayed Ahmed, *The Legal Protection of Personal Data (A Comparative Study of British and Emirati Law)*, *Journal of Judiciary and Law*, Judicial Department, No. 04, Abu Dhabi, 2018.
3. Belafred Latti Lamine and Amhend Barkaouk, *Cyberspace: Actors and Threats*, *Afaq Journal of Sciences*, No. 03, University of Ziane Achour, Djelfa, Algeria, 2024.
4. Alaa Eddine Farhat, *Cyberspace: Shaping the Battlefield of the 21st Century*, *Journal of Legal and Political Sciences*, No. 03, University of Algiers 1, Algeria, 2019.
5. Ramadan Ben Khamma, *Children and Social Media Networks: Challenges, Risks, and Mechanisms of Protection and Guidance – A Theoretical Approach*, *Al-Mi'yar Journal*, No. 03, University of Tissemsilt, Algeria, 2022.
6. Bertrand Boyer, *Cyberstrategie: L'art de la guerre numérique*, Paris: NUNIS, 2012.
7. Bertrand Boyer, *Cyberstrategie: Conduire la guerre numérique*, Paris: NUNIS, 2014.
8. N. Nciri, "Access to Administrative Documents in Tunisia", in *Democracy and Administration*, Proceedings of the Conference held in Tunis on October 10–11, 2011, Faculty of Law and Political Science of Tunis, Latrach Editions, Tunis, 2014.
9. Organization for Economic Co-operation and Development (OECD), *Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (2013) [C(80)58/FINAL, as amended on July 11, 2013 by C(2013)79].