PROTECTION OF PERSONAL DATA FOR CONSUMERS IN E-COMMERCE A STUDY IN LIGHT OF LAW NO. 18-07

FTISSI FOUZIA[1]

[1]Lecturer Class A, Faculty of Law and Political Science, Department of Law, Laboratory of Environmental Legal Studies, University of May 8, 1945 - Guelma (Algeria).

The E-mail Author: ftissi.fouzia@univ-guelma.dz

Received: 16/07/2023 **Published: 03/03/2024**

Abstract:

Most legislations in various countries around the world seek to protect individuals' private lives by establishing an effective legal framework to achieve this goal. This is especially necessary to keep pace with developments in commercial transactions, which are increasingly conducted electronically and require attention to the privacy of this type of transaction. In this regard, the importance of protecting personal data emerges. Hence, Algeria issued Law No. 18-07, dated June 10, 2018, concerning the protection of personal data, which is considered an important step towards enhancing trust in e-commerce in Algeria.

Keywords: *consumer, e-commerce, personal data, legal protection.*

INTRODUCTION:

E-commerce, in light of rapid technological advancement, has become an integral part of our daily lives, with billions of commercial transactions conducted online annually. With this significant growth, the importance of protecting consumers' personal data has emerged as one of the most critical rights in the evolving digital age. The exchange of this data online has become indispensable for electronic buying and selling of all products, which exposes this data to various threats, such as cyber breaches, electronic fraud, and identity theft. This necessitates the establishment of an effective legal framework to ensure its protection.

In the context of e-commerce and the increase in online business activities, protecting consumers' personal data is of paramount importance. A vast amount of data is collected, including names, addresses, phone numbers, passwords, codes, financial information, among others. This data can be used unethically or illegally, and it is natural for issues to escalate as a result of these uses and the sharing of this data online, exposing consumers to serious risks.

In this regard, many countries have enacted legislation and laws to protect personal data and regulate its transactions. Law No. 18-07, dated June 10, 2018[1], is one of the most significant legislations that govern the protection of personal data in Algeria. It aims to ensure individuals' rights to control their personal data and provide a safe environment for e-commerce, especially amid the significant expansion of internet and e-commerce usage. In this context, the following issue can be raised:

Has the Algerian legislator, through Law 18-07 concerning the protection of personal data, established a sufficient and effective legal framework to protect consumers' private data and enhance trust in e-commerce transactions?

To address the posed issue, we relied on both the descriptive approach and content analysis methodology as required by the study, following the division outlined below:

First: Conceptual Definitions of the Study Variables

1- Law No. 18-07, dated June 10, 2018, concerning the protection of natural persons in the field of personal data processing, Official Gazette of the People's Democratic Republic of Algeria, No. 34, dated June 10, 2018.

Second: Fundamental Principles of Personal Data Protection

Third: Legal Controls for Personal Data Protection

Fourth: The National Authority as a Mechanism for Protecting Private Data

First: Conceptual Definitions of the Study Variables

To gain a good understanding of the topic, it was necessary to define the variables of the study, which we will attempt to address in the following:

1. Definition of Personal Data:

Personal data is defined as "information through which a natural or legal person can be identified, specifically relating to the individual concerned, who can be identified directly or indirectly.[1]" It is generally defined as "personal identification information exchanged over the internet.[2]"

The European Convention No. 108 defines personal data as 'any information relating to the identification of an individual, or to a specific individual'. In Law 18-07, dated 10 June 2018, concerning the protection of natural persons in the processing of personal data, the Algerian legislator defined personal data as "any information relating to an identified or identifiable natural person, referred to hereinafter as the 'data subject', which can be used to directly or indirectly identify that person, particularly by reference to an identification number or to one or more factors specific to their physical, physiological, genetic, mental, economic, cultural or social identity"[3]. In this context, the 'data subject' refers to 'any natural person whose personal data is subject to processing'. Meanwhile, the Tunisian legislator defined it as follows: '... any data, regardless of its source or form, that identifies or could identify a natural person, either directly or indirectly, with the exception of information relating to public life or that is considered as such by law.[4]'

Clearly, personal data only has value when it pertains to a specific individual whose identity can be verified, for example, using a national identification number. This can contribute to our understanding of the individual's regional affiliation. Associating information with a person makes it personal data. For example, a home address has no value as regular data, but when linked to a specific person, it can provide identifying information about them. In this case, it is considered personal data.

The Office of Management and Budget memorandum from the White House defines personal data as 'any information that can be used to distinguish or trace the identity of an individual, such as a name, social security number or biometric records, or any other information relating to or associated with a specific person, such as a date or place of birth or mother's maiden name'[5].

Thus, it is clear that data protection only pertains to natural persons, not legal persons, and only when they are defined or identifiable by distinguishing traits related to their physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity, or any other characteristic that allows for their identification[6].

1- Abdul Latif Al-Rami, "Protection of Consumers' Personal Data in Electronic Commerce," Your Law Journal, No. 17, 2023, p. 231.

2- Aliya Ali Zakaria Ali, "Protection of Sensitive Medical Personal Data from the Perspective of Evolving Health Rights Protection - A Comparative Study," Spirit of Laws Journal, Faculty of Law, Vol. 1, No. 104, October 2023, p. 178.

3- See Article 3 of Law 18-07, mentioned above.

4- Tunisian Fundamental Law, No. 63, dated July 27, 2004, concerning the protection of personal data, Article 4, p. 2.

5- Abdul Latif Al-Rami, Previous Reference, p. 231.

6- Naziha Ben Allal, "The Legal Framework for Protecting Personal Data in Cyberspace Under Law No. 18-07," Journal of Legal and Political Research and Studies, Vol. 4, No. 2, 2020, p. 56.

2. Definition of the consumer:

Law No. 04-02 concerning commercial[1] practices defines the consumer in Article 3(2) as 'any natural or legal person who acquires goods offered for sale or benefits from services provided, devoid of any professional character'. Subsequently, Law No. 09-03 concerning consumer protection and fraud suppression[2] further refines this definition in Article 3(2) to include "any natural or legal person who acquires, for a fee or free of charge, goods or services intended for final use to meet their personal needs, or the needs of another person or animal under their care". Thus, the Algerian legislator has adopted a narrow definition of the consumer, excluding professionals.

Law No. 18-05 on e-commerce defines an electronic consumer[3] in Article 6(3) as 'any natural or legal person who, for a fee or free of charge, acquires a good or service through electronic communications from an electronic supplier for final use'.

3. Definition of E-Commerce:

E-commerce is defined as 'the steps involved in the buying, selling and exchanging of goods, services and information over computer networks'[4]. The World Trade Organization defines it as 'activities related to the production, distribution, marketing, sale or delivery of goods and services to buyers through electronic means'[5].

In Law No. 18-05 concerning e-commerce, the Algerian legislator defines it in Article 6(1) as 'the activity whereby an electronic supplier proposes or ensures the provision of goods and services remotely to an electronic consumer through electronic communications'.

Second: Fundamental Principles of Personal Data Protection

To ensure the integrity of the processing of personal data, the Algerian legislator set out a number of principles in Chapter Two of Law No. 18-07. We will discuss these principles below:

1. Prior consent and data quality:

According to Article 7 of Law 18-07, the data processor can only carry out processing with the explicit consent of the data subject. Article 3 of Law 18-07 defines consent as 'any distinct expression of will by which the data subject or their legal representative agrees to the processing of personal data relating to them, whether manually or electronically'.

In accordance with Article 7, if the data subject is incompetent or partially competent, this consent is subject to the rules set out in general law. The data subject may withdraw their consent at any time. As a general principle, third parties cannot access personal data subject to processing, except for purposes directly related to the tasks of the data processor and the recipient, and only after obtaining prior consent from the data subject. However, consent is not required if processing is necessary to comply with a legal obligation applicable to the data subject or data processor; to protect the life of the data subject; to fulfil a contract to which the data subject is a party; to carry out pre-contractual measures taken at the data subject's request; or to safeguard vital interests if the data subject is physically or legally unable to express consent. Consent may also be given to fulfil a task in the public interest or in the exercise of public authority vested in the data processor or third party informed of the data; or to achieve a legitimate interest of the data processor or recipient,

[1]- Law No. 04-02, dated June 23, 2004, defining the rules applicable to commercial practice, Official Gazette of the People's Democratic Republic of Algeria, No. 41, dated June 27, 2004.
[2]- Law No. 09-03, dated February 25, 2009, concerning consumer protection and the suppression of fraud, Official Gazette of the People's Democratic Republic of Algeria, No. 15, dated March 8, 2009.
[3]- Law No. 18-05, dated May 10, 2018, concerning electronic commerce, Official Gazette of the People's Democratic Republic of Algeria, No. 28, dated May 16, 2018.
[4]- Muhammad Nour Saleh Al-Jidaya and Sana'a Joudat Khalaf, Electronic Commerce, Dar Al-Hamid for Publishing and Distribution, Amman, 2nd Edition, 2012, p. 24.
[5]- Ibrahim Al-Eisawi, Electronic Commerce, Academic Library, Cairo, 2003, p. 31.

provided that the interests and/or fundamental rights and freedoms of the data subject are not overridden.

In cases where the data subject is a child, processing of their personal data can only occur after consent has been obtained from their legal representative, unless permission has been granted by a competent judge. A judge may authorise processing without the consent of the child's legal representative if it is in the child's best interests, and may revoke their authorisation at any time[1].

It is important to note that the right to withdraw explicit consent poses a significant threat to the stability of transactions. To prevent abuse of the right to withdraw, it would be prudent to make this right conditional upon legitimate reasons, or to make it an automatic right once the required retention period has expired or the purpose for which the personal data was requested has been completed. The legislator should reconsider the wording of Article 7 of Law 18-07 regarding the prior consent of the data subject, as mere explicit consent is insufficient. Consent must be clear, informed and conscious to ensure it is well considered, particularly in a digital environment where it may be subject to unclear technical methods[2].

In terms of data quality, the legislator has stipulated that personal data must be processed lawfully and fairly. It must be collected for specific, clear and legitimate purposes and not processed in a way that is incompatible with these purposes. The data must be adequate, relevant and not excessive in relation to the purposes for which it was collected or processed. The data must also be accurate and complete, and kept up to date where necessary. It must be stored in a way that allows for the identification of the data subjects, but only for as long as is necessary to achieve the purposes for which it was collected and processed. Upon request from the data processor and in the presence of a legitimate interest, the national authority may allow the retention of personal data for historical, statistical, or scientific purposes beyond the aforementioned period[3].

Article 10 of the same law limits the processing of data relating to crimes, penalties, and security measures to the judiciary, public authorities, legal entities managing public interests, and justice assistants within their respective legal competencies. The article outlines measures to ensure the security of the processing and requires the processor, the purpose of the processing, the data subjects involved, third parties entitled to access this information and its sources, and the necessary procedures to be clearly defined.

Judicial rulings that require an assessment of an individual's behaviour cannot be based solely on the automated processing of personal data, including the evaluation of certain aspects of their personality. Similarly, no decision with legal consequences for a person can be made based solely on the automated processing of data aimed at determining the characteristics of the data subject or assessing certain aspects of their personality. However, decisions made in the context of concluding or executing a contract where the data subject has been given the opportunity to provide feedback, and decisions made in response to requests from the data subject, are not considered to be based solely on automated processing[4].

2. Preliminary procedures for processing:

The law requires certain preliminary procedures to be completed before any personal data can be processed. These procedures include:

2.1. Declaration:

1- See Article 8 of Law 18-07, mentioned above.
2- Jawhar Gwadri Samit, "Legal Controls for Processing Personal Data Electronically," Journal of Comparative Legal Studies, Vol. 06, No. 02, 2020, p. 476.
3- See Article 9 of Law 18-07, mentioned above.
4- See Article 11 of Law 18-07, mentioned above.

The first of these procedures is to submit a declaration to the relevant authority, as set out in Article 12 of Law 18-07. This article states: 'Unless otherwise provided for by law, all processing of personal data is subject to prior declaration to, or authorisation by, the national authority, in accordance with the provisions of this law.'

The declaration can be submitted to the national authority in either conventional or electronic form. The declaration commits the data processor to carrying out the processing in accordance with the law. They may not commence processing until they have received confirmation of receipt of the declaration, which must be issued or sent immediately or within a maximum of 48 hours, in either conventional or electronic form. The data processor may include all processing activities related to the same purpose or related purposes under a single declaration[1]. Thus, it is clear that the prior declaration merely notifies the national authority that the data processor intends to proceed with the operation, allowing the declarant to start their work upon receiving the receipt[2].

According to Article 14 of Law 18-07, this declaration must include the following details: the name and address of the data processor; the name and address of their representative (where applicable); the nature and characteristics of the processing; the purpose of the processing; a description of the category or categories of data subjects; the personal data or categories of personal data concerning the data subjects; the recipients who may receive the data; the nature of the data intended to be sent to foreign countries; and the duration of data retention. Any changes to the information mentioned in this Article, or any deletions affecting the processing, must be notified to the national authority immediately.

According to Article 17 of the same law, if, upon reviewing the submitted declaration, the national authority finds that the intended processing poses significant risks to the respect and protection of privacy and the fundamental rights and freedoms of individuals, it may decide to subject the processing to a prior authorisation regime. This decision will be communicated to the data processor within ten days of the declaration being submitted.

2.2. Authorization:

Authorization means granting the national authority's explicit consent to carry out processing operations concerning sensitive data, which is generally prohibited by law. However, the national authority may exceptionally grant authorization to the data processor in certain specific cases[3], by means of a decision made within two months from the date of notification. This period can be extended for the same duration by a reasoned decision from its president. A failure to respond within the specified time frame is considered a rejection of the request[4]. It is emphasized that the authorization request must include the same information mentioned in Article 14. In this case, the declarant is obligated not to carry out the processing operation due to the national authority's lack of approval.

Third: Legal Controls for Personal Data Protection

We will address these controls through the obligations of the data processor and the rights of the data subjects, as follows:

1. Obligations of the Data Processor Regarding Personal Data Processing:

Law 18-07 imposes several specific obligations on the data processor, which include:

1- See Article 13 of Law 18-07, mentioned above.
2- Jawhar Gwadri Samit, Previous Reference, p. 471.
3- For determining those cases, see Article 18 of Law 18-07, mentioned above.
4- See Article 20 of the same law.

1.1. Obligations to Ensure the Integrity and Confidentiality of the Processing:

The data processor must take a series of appropriate technical and organizational measures to protect personal data from accidental or unlawful destruction, accidental loss, damage, publication, or unauthorized access, especially when processing requires sending data over a specific network. They must also protect it from any form of unlawful processing, ensuring these measures provide an appropriate level of security relative to the risks posed by processing and the nature of the data to be protected, in accordance with Article 38 of Law 18-07.

When processing is carried out on behalf of the data processor, the latter must choose a subcontractor who provides adequate guarantees regarding the technical and organizational safety procedures that need to be implemented and ensures compliance with them. The subcontracting process must be organized by a contract or legal document binding the subcontractor to the data processor, which specifically stipulates that the subcontractor may only act on the instructions of the data processor and must comply with the obligations outlined in Article 38. For evidentiary purposes, all elements of the contract or legal document concerning data protection, as well as the requirements related to the measures in Article 38(1), must be documented in writing or in another equivalent form[1].

The data processor and individuals who, in the course of their duties, access personal data are bound by professional secrecy and must not disclose any information they have accessed, even after their duties have ended, under penalty of the sanctions outlined in applicable legislation, as per Article 40 of the same law. Additionally, no person working under the authority of the data processor or the authority of the subcontractor who accesses personal data may process this data without the data processor's instructions, except in the case of fulfilling a legal obligation[2].

It is noteworthy that the legislator has linked the obligation of confidentiality to the obligation of security, as they are complementary. In order to guarantee the integrity of the processing, the data processor must implement the necessary measures and procedures to achieve this, establishing rules and limits on access to the data, even for the processors, so that they only have access to what is necessary for the performance of their respective tasks. In addition, special programmes must be used to prevent breaches and unauthorised access to each file, using techniques that restrict access to those who do not have the right to see it, thereby providing protection against any alteration or deletion of information[3].

1.2. Processing of personal data in the field of electronic certification and signatures and electronic communications:

Personal data collected by electronic certification service providers for the purpose of issuing and maintaining certificates related to electronic signatures must be obtained directly from the data subjects. Such data may not be processed for purposes other than those for which they were collected, except with the explicit consent of the data subject[4].

If the processing of data in open electronic communications networks leads to their destruction, loss, disclosure or unauthorised access, the service provider must immediately inform the national authority and the data subject if such incidents affect their privacy, unless the national authority determines that the necessary data protection safeguards have been implemented by the service provider. Each service provider must maintain an up-to-date record of personal data breaches and the actions taken in response[5].

1.3. Transfer of information abroad:

1- See Article 39 of Law 18-07, mentioned above..
2- See Article 41 of the same law.
3- Jawhar Gwadri Samit, Previous Reference, p. 473.
4- See Article 42 of Law 18-07, mentioned above.
5- See Article 43 of Law 18-07, mentioned above.

The data processor may not transfer personal data abroad without the authorisation of the national authority in accordance with the provisions of this Act. Such a transfer is permitted only if the foreign country ensures an adequate level of protection of the privacy and fundamental rights and freedoms of individuals with regard to the processing or potential processing of such data. The national authority shall assess the adequacy of the level of protection provided by a particular country, in particular in relation to the applicable legal requirements and security measures enforced there, as well as the characteristics of the processing, such as its purpose, duration, nature, origin and destination of the processed data. In all cases, the transfer of personal data abroad is prohibited if it may jeopardise public security or the vital interests of the State[1].

Notwithstanding the foregoing provisions, the data controller may transfer personal data to a country that does not fulfil the conditions set out in Article 44, under the specific circumstances set out in Article 45 of the same Code. These circumstances include, first, the explicit consent of the data subject; second, if the transfer is necessary to protect the life of the data subject, to serve the public interest, to fulfil obligations that guarantee the establishment or exercise of a right or defence in legal proceedings, to execute a contract between the processor and the data subject or to carry out pre-contractual measures taken at the request of the data subject, to conclude or execute a contract between the processor and a third party for the benefit of the data subject, to carry out actions related to international judicial cooperation or for the prevention, diagnosis or treatment of diseases; and third, if the transfer is made pursuant to a bilateral or multilateral agreement to which Algeria is a party; and fourth, on the basis of an authorization by the national authority, if the processing is in conformity with the provisions of Article 2 of this law.

2. Rights of the data subject with regard to the processing of his personal data:

Law 18-07 establishes several rights for the data subject in order to enable them to control their personal data. These rights include the right to be informed, the right to access, the right to object, the right to rectify and the right to prevent direct research.

2.1. Right to Information:

The legislator, through Article 32 of Law 18-07, obligates the data processor or their representative to inform every individual contacted for the purpose of collecting their personal data in advance, clearly, and unambiguously, unless they are already aware of the following elements:

- The identity of the data processor and, where applicable, the identity of their representative,

- The purposes of the processing,

- Any additional useful information, particularly the recipients of the data, the obligation to respond, the consequences of that response, and the rights of the individual, including the transfer of data to a foreign country...

If personal data is not collected directly from the data subject, the data processor or their representative must provide the aforementioned information before recording or sharing it with others, unless the individual has already been informed.

Where information is collected over open networks, the data subject must be informed, unless they are already aware that their personal data may be shared over networks without safety guarantees and may be subject to unauthorised reading and use by others.

Article 33 of the same law provides an exception to the obligation to inform outlined in Article 32, stating that the obligation does not apply in the following cases:

[1]- See Article 44 of Law 18-07, mentioned above.

If it is impossible to inform the data subject, especially when personal data is processed for statistical, historical or scientific purposes. In this case, the data processor must notify the national authority of the impossibility of informing the data subject and provide reasons for this impossibility.

If the processing is carried out in accordance with a legal provision.

- if the processing is exclusively for journalistic, artistic or literary purposes.

2.2. Right of access:

This right, established under Article 34 of Law 18-07, allows the data subject to obtain the following from the data processor:

- confirmation that their data has been processed, including the purposes of processing, the categories of data involved and the recipients;

- Access to their personal data being processed, along with any available information regarding the source of the data, provided in an understandable format.

In return, the data processor has the right to ask the national authority to set deadlines for responding to legitimate requests for access and may object to unreasonable requests, in particular with regard to their nature and frequency, bearing the burden of proof for such claims.

2.3. Right of rectification:

Article 35 grants the data subject the right to obtain from the data processor, free of charge, the updating, rectification or erasure of the data:

- The updating, rectification, erasure or blocking of personal data processed in breach of the law because they are incomplete or inaccurate or because their processing is prohibited by law. The data processor is obliged to make the necessary corrections free of charge within ten (10) days of notification. If the request is refused or not responded to within the prescribed period, the data subject has the right to submit a request for rectification to the national authority, which will appoint a member to carry out all the necessary investigations and make the necessary corrections as soon as possible, informing the data subject of the outcome of his or her request.

- Notify any third party who has received the personal data of any update, correction, deletion or blocking, unless this is impossible.

The law also allows the exercise of this right by the heirs of the data subject.

2.4. Right to object:

Through article 36 of law 18-07, the Algerian legislator grants the data subject the right to object, for legitimate reasons, to the processing of his personal data. They also have the right to object to the use of their data by the current or a subsequent data processor for advertising purposes, particularly commercial.

However, the data subject may not object to the processing of his or her personal data for legitimate reasons if the processing is necessary to fulfil a legal obligation or if the application of these provisions has been expressly excluded in the document authorising the processing.

2.5. Prohibition of Direct Solicitation:

Article 37 of Law 18-07 prohibits direct solicitation through any means of communication or remote copying device, email, or any technology of a similar nature, using the personal data of an individual in any form without their prior consent.

However, direct solicitation via email is permitted if the data is requested directly from the recipient, in accordance with the provisions of the law, regarding the sale or provision of services, provided that the direct solicitation pertains to similar products or services offered by the same individual or

legal entity. The recipient must be clearly informed of their ability to object without incurring costs, except for the expenses related to sending the rejection, at the time their data is collected and whenever they receive an email for solicitation purposes.

In all cases, sending messages via telecommunication devices, remote copying devices, and email for direct solicitation is prohibited without providing accurate data to enable the recipient to send a request to stop these communications without any costs other than those related to sending them.

Additionally, concealing the identity of the person for whom the messages were sent is prohibited, as is mentioning a subject unrelated to the services offered.

Fourth: The National Authority as a Mechanism for Protecting Personal Data

The Algerian legislator established an institutional mechanism for protecting personal data through Law 18-07.

Through the aforementioned Law 18-07, the Algerian legislator established an institutional mechanism for protecting personal data. We will discuss its establishment, structure and functions below:

1. Establishment and structure of the National Authority for the Protection of Personal Data:

Article 22 of Law 18-07 stipulates the creation of an independent administrative authority for the protection of personal data. This authority is called the National Authority and is based in Algiers. The National Authority enjoys legal personality and financial and administrative independence. Its budget is included in the state budget and is subject to financial oversight in accordance with applicable legislation. The National Authority is responsible for drafting its internal regulations, which specifically outline its organisation and operation, and must approve them.

According to Article 23 of the same law, the National Authority comprises the following members:

Three individuals, including the president, chosen by the President of the Republic from among those with expertise in the field of the National Authority's work;

Three judges proposed by the Supreme Judicial Council from among the judges of the Supreme Court and the Council of State;

- one member from each chamber of parliament, chosen by the president of each chamber after consulting the parliamentary group leaders;

- one representative from the National Council for Human Rights;

- one representative from the Minister of National Defence;

- one representative from the Minister of Foreign Affairs;

- One representative from the Minister responsible for Interior Affairs;

- One representative from the Minister of Justice and Keeper of the Seals;

- One representative from the Minister responsible for Postal Services, Telecommunications, Technology and Digitalisation;

- One representative from the Minister of Health;

- One representative from the Minister of Labour, Employment and Social Security.

The members of the National Authority shall be selected on the basis of their legal or technical expertise in the field of personal data processing. The National Authority may call upon any qualified person to assist it in its work. The President and the members of the authority are appointed by presidential decree for a renewable term of five (5) years.

2. Tasks of the National Authority for the Protection of Personal Data:

The National Authority is tasked, under Article 25 of Law 18-07, with ensuring that the processing of personal data complies with the provisions of this law and that the use of information and communication technologies does not pose any risks to individuals' rights, public freedoms, and private life. In this regard, its tasks include, in particular:

- Granting licenses and receiving declarations related to the processing of personal data,

- Informing data subjects and data processors of their rights and obligations,

- Providing consultations to individuals and entities engaged in the processing of personal data or conducting experiments or practices that may lead to such processing,

- Receiving objections, appeals, and complaints regarding the implementation of personal data processing and informing the parties involved of the outcomes,

- Authorizing the transfer of personal data abroad in accordance with the conditions set forth in this law,

- Ordering necessary changes to protect processed personal data,

- Ordering the closure, withdrawal, or destruction of data,

- Proposing any measures to simplify and improve the legislative and regulatory framework for personal data processing,

- Publishing granted licenses and opinions in the national register mentioned in Article 28 of this law,

- Developing cooperative relationships with similar foreign authorities, taking reciprocity into account,

- Imposing administrative penalties in accordance with the provisions of Article 46 of this law,

- Establishing standards in the field of personal data protection,

- Establishing codes of conduct and ethics governing personal data processing.

Upon observing such occurrences, the National Authority must immediately inform the competent public prosecutor of any facts that may warrant criminal charges. It is also required to prepare an annual report on its activities for submission to the President of the Republic.

CONCLUSION:

Law 18-07 is an important step towards building trust in e-commerce in Algeria by providing a comprehensive legal framework for protecting personal data. It reflects efforts to keep pace with technological developments and ensure individuals' rights to privacy and digital security, thereby contributing to the establishment of a secure and sustainable digital economy. However, raising awareness and ensuring effective implementation remain key challenges that need to be addressed.

First: Findings

- The Algerian legislator has established a set of basic principles for the protection of personal data.

- The legislator has imposed a number of obligations on data processors, including preliminary procedures for processing (declaration and prior authorisation, explicit consent of the data subject) and the obligation to ensure the integrity and confidentiality of processed data.

- A number of rights have been recognised for individuals whose data are processed, including the right to be informed, the right of access, the right to object, the right to rectify and the right to prevent direct marketing.

- Through Law 18-07, the Algerian legislator has created an independent administrative authority as a mechanism for the protection of personal data, known as the National Authority, which has been entrusted with a number of tasks.

Second: Proposals

- Establish and activate the institutional mechanism defined by the Algerian legislator in law 18-07, represented by the National Authority for the protection of natural persons with regard to their personal data against various violations.

- Selecting individuals responsible for data processing who are qualified (technically), trustworthy and of high ethical standards to ensure data confidentiality and privacy.

- Utilise the latest technologies and expertise from developed countries in the field of personal data processing.

- In order to ensure the free flow of data across borders, it is essential to coordinate between countries to achieve harmony between protection laws, thereby protecting citizens.

LIST OF SOURCES AND REFERENCES:

First: Sources

- Law No. 04-02, dated 23 June 2004, defining the applicable rules of commercial practice (Official Gazette of the People's Democratic Republic of Algeria, No. 41, dated 27 June 2004).

Tunisian Fundamental Law No. 63, dated 27 July 2004, relating to the protection of personal data (Article 4).

Law No. 09-03 dated 25 February 2009 concerning consumer protection and the suppression of fraud (Official Gazette of the People's Democratic Republic of Algeria No. 15 dated 8 March 2009).

Law No. 18-05 dated 10 May 2018 related to electronic commerce (Official Gazette of the People's Democratic Republic of Algeria, No. 28 dated 16 May 2018).

Law No. 18-07 dated 10 June 2018 concerning the protection of natural persons in the field of personal data processing (Official Gazette of the People's Democratic Republic of Algeria No. 34 dated 10 June 2018).

Second: References

1. Books:

Ibrahim Al-Aissawi, Electronic Commerce, Academic Library, Cairo, 2003.

Mohammad Nour Saleh Al-Jidaya and Sana'a Joudat Khalaf, Electronic Commerce, Dar Al-Hamid for Publishing and Distribution, Amman, 2nd edition, 2012.

2. Articles:

Jawhar Gouadri Samit, 'Legal Controls for Processing Personal Data Electronically', Journal of Comparative Legal Studies, Vol. 6, No. 2, 2020.

Abdul Latif Al-Rami, 'Protection of Consumers' Personal Data in Electronic Commerce', Your Law Journal, No. 17, 2023.

- Aliya Zakaria, 'Protection of Sensitive Medical Personal Data from the Perspective of Evolving Health Rights Protection: A Comparative Study', Spirit of Laws Journal, Faculty of Law, Vol. 1, No. 104, October 2023.

Naziha Ben Allal: 'The Legal Framework for Protecting Personal Data in Cyberspace under Law No. 18-07', Journal of Legal and Political Research and Studies, Vol. 4, No. 2, 2020.