Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

Legal Protection of the Personal Data of the Electronic Consumer in Electronic Commerce Contracts under Algerian Legislation

Dr. Mohammed Abib
Private Law (Advanced) – University of Tissemsilt
E-mail: abib.mohammed@cuniv-tissemsilt.dz

Received: 20/01/2026 Accepted:02/03/2026 Published: 05/08/2026

Abstract
The parties to an electronic commerce contract—the electronic supplier and the electronic consumer—are required, for the execution of the contract, to provide their essential personal data within the digital environment. Such data may be exposed to serious infringements affecting the consumer's privacy, whether by third parties or even by the electronic supplier himself. Consequently, legislations around the world have established the necessity of subjecting the processing of personal data to legal restrictions in order to ensure the protection of personal data during automated processing, as well as to guarantee its security and proper circulation, thereby promoting the safe conduct of electronic commerce activities. In this regard, the Algerian legislator has imposed a set of obligations in accordance with the applicable legislation and regulations, particularly Law No. 18-07 relating to the protection of natural persons with regard to the processing of personal data, as well as Law No. 18-05 on electronic commerce, especially the provisions of Article 26, which constitute the legal and legitimate basis governing this matter.
Keywords: Electronic commerce contract, electronic supplier, electronic consumer, protection of personal data.

Introduction

The protection of personal data is considered a matter of paramount importance and has become a central concern of legislations worldwide. These legislations have sought to ensure such protection because of its fundamental role in establishing a secure digital environment and strengthening trust, thereby contributing to the promotion and growth of electronic commerce. The protection of personal data also falls within the broader framework of the protection of human rights and fundamental freedoms. In this regard, during its session held on 24 October 1995, the European Parliament adopted the important Directive 95/46/EC, concerning the protection of individuals with regard to the processing of personal data and the free movement of such data. The Directive required all Member States to enact legislation protecting personal data or to amend their existing legislation so as to comply with its provisions.[1]

The Algerian legislator constitutionally enshrined the right to the protection of personal data in the field of personal data processing under the last paragraph of Article 46 of the 2016

[1] Karim Seffar, La régulation du commerce électronique global, Doctoral Thesis, Faculty of Graduate Studies, University of Montreal, 2013, p. 238.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

Constitution.[1] This guarantee was reaffirmed in the 2020 Constitution, specifically in the last paragraph of Article 47, which provides that the protection of personal data constitutes a fundamental right, the violation of which is punishable by law. This constitutional protection was implemented through Law No. 18-07 on the Protection of Natural Persons with Regard to the Processing of Personal Data.[2] Furthermore, the electronic consumer's right to the protection of personal data vis-à-vis the electronic supplier within the framework of an electronic commerce contract was recognized by Law No. 18-05 on Electronic Commerce,[3] particularly under Article 26, which obliges the electronic supplier to comply with a set of legal and regulatory requirements, especially those governing the processing of the electronic consumer's personal data in electronic commerce contracts.

Section One: The Electronic Supplier’s Obligation to Protect the Personal Data of the Electronic Consumer in the Electronic Commerce Contract

First Requirement: Controls Governing the Automated Processing of Personal Data in the Electronic Commerce Contract

The Nature of Personal Data in the Electronic Commerce Contract

1. Definition of Personal Data

Although the task of formulating legal definitions is generally entrusted to legal scholars and the judiciary, legislators sometimes provide statutory definitions because of their paramount importance in clarifying concepts and determining the precise meaning of terms that may often overlap and therefore require accurate interpretation.

The Egyptian legislator defined personal data in Article 1 of the Personal Data Protection Law as: "Any data relating to an identified or identifiable natural person, whether directly or indirectly identifiable through the linkage of such data with other data, such as a name, voice, image, identification number, online identifier, or any data revealing the person's psychological, health, economic, or social identity."[4]

Likewise, the French legislator adopted the definition contained in Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data. Accordingly, the French Data Protection Act (Informatique et Libertés) was amended by Law No. 2018-493 of 20 June 2018 on personal data protection. Article 4 thereof defines personal data as any information relating to an identified or identifiable natural person, hereinafter referred to as the data subject. An identifiable natural person is one who can be identified, directly or indirectly, particularly by reference to an identifier such as a name,

---

[1] Law No. 16-01 concerning the Constitutional Amendment, dated 6 March 2016, Official Gazette of the People's Democratic Republic of Algeria, No. 14, issued on 7 March 2016, Article 46.

[2] Law No. 18-07 on the Protection of Natural Persons with Regard to the Processing of Personal Data, Official Gazette No. 34, issued on 10 June 2018.

[3] Law No. 18-05 on Electronic Commerce, dated 10 May 2018, Official Gazette No. 28, issued on 16 May 2018.

[4] Ayman Mostafa Ahmed Al-Baqli, Protection of Informational Privacy in Light of the Requirements of Electronic Commerce, Legal Journal, Faculty of Law, University of Khartoum, No. 4, 2021, p. 1030.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

identification number, location data, online identifier, or one or more factors specific to the person's physical, physiological, genetic, mental, economic, cultural, or social identity.[1]

It is evident that this definition is broad, precise, and contemporary, encompassing every element capable of identifying an individual in any manner.

Similarly, the Algerian legislator defined personal data in Article 3, Paragraph 1 of Law No. 18-07 as any information, regardless of its medium, relating to an identified or identifiable person, hereinafter referred to as the data subject, whether identified directly or indirectly, particularly by reference to an identification number or one or more elements specific to his or her physical, physiological, genetic, biometric, psychological, economic, cultural, or social identity. This definition was clearly inspired by the aforementioned European Union Regulation.

2. Automated Processing of Personal Data in the Electronic Commerce Contract

Article 26 of the Electronic Commerce Law refers to the legislation governing the protection of personal data, namely Law No. 18-07 on the Protection of Natural Persons with Regard to the Processing of Personal Data. Article 3, paragraph 3, of this Law defines the processing of personal data as any operation or set of operations performed, whether by automated means or otherwise, on personal data.

Such operations include collection, recording, organization, disclosure, modification, extraction, consultation, use, communication by transmission, dissemination, or any other form of making the data available, alignment, interconnection, blocking, encryption, erasure, or destruction.

Furthermore, paragraph 5 of the same article defines automated processing as any operation or set of operations carried out wholly or partially by automated means, or otherwise, on personal data, including collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination, or any other form of making the data available, alignment, interconnection, blocking, encryption, erasure, or destruction.[2]

3. Justifications for Establishing the Electronic Supplier's Obligation to Protect the Personal Data of the Electronic Consumer

There are several justifications for establishing the electronic supplier's obligation to protect the personal data of the electronic consumer. The most significant of these are the risks associated with the digital environment and the need to strengthen trust in electronic commerce.

The risks inherent in the digital environment arise from the disclosure of consumers' personal data during electronic contracting. Such disclosure places personal data within a digital environment, transforming it into electronic data that becomes vulnerable to various risks resulting from information and communication technologies. This is due to the enormous technical capabilities of the digital environment, the extent and impact of which cannot always

[1] Ibid., p. 1032.

[2] Article 3 of Law No. 18-07 on the Protection of Natural Persons with Regard to the Processing of Personal Data, Official Gazette No. 34, issued on 10 June 2018.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 2,* 2026
Website: https://ceapress.org

be anticipated.[1] Consequently, it has become necessary for legislatures to establish legal rules that reinforce trust in electronic commerce. Trust constitutes one of the most important legal guarantees for ensuring the stability of commercial transactions in the digital environment. One of the principal manifestations of promoting such trust is the imposition of an obligation to ensure the security and integrity of consumers' personal data.

The exchange of electronic information provides numerous advantages, particularly speed, as it eliminates delays in processing order-related information that are typically associated with traditional postal services. It also reduces costs. In addition, its most significant advantage lies in ensuring security and confidentiality, as electronic information exchange offers a higher level of protection for confidential information than that available through conventional means of communication.[2]

Conditions Governing the Automated Processing of Personal Data in Electronic Commerce Contracts

The European Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, together with European Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, established several fundamental principles governing the processing of personal data. With regard to the principle of collecting and processing personal data, Articles 5, 6, and 9 of the European Convention stipulate that personal data subject to automated processing must be obtained and processed fairly and lawfully, stored for specified and legitimate purposes, and not used in a manner incompatible with those purposes.[3]

Similarly, Article 9 of Algerian Law No. 18-07 concerning the protection of natural persons in the processing of personal data sets forth a number of conditions that must be observed. In particular, personal data must be processed in a lawful and fair manner.

Personal data must be processed fairly and lawfully. This means that information should be processed on the basis of a clear legal foundation, for legitimate purposes, and in a fair and transparent manner, enabling users to be adequately informed about how their personal data are collected, used, or stored, as well as the entity responsible for such processing.[4]

The Algerian legislator has emphasized the protection of personal data, whether under Article 9 of Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data or Article 26 of the Electronic Commerce Law, which constitutes the legal basis governing this matter. Accordingly, the purpose of data processing must be clearly specified. Personal data may only be collected and processed for a specific, explicit, and legitimate purpose. Within the

[1] Seham Qaroun, "The Electronic Supplier's Obligation to Protect Consumers' Personal Data under Law No. 18-05 on Electronic Commerce," Al-Bahith Journal for Academic Studies, Faculty of Law and Political Science, Hadj Lakhdar University, Batna 1, Vol. 7, No. 2, June 2020, p. 1017.
[2] Jean-Pierre Clavier & Alexandra Mendoza-Caminade, op. cit., p. 126.
[3] Marwa Zain Al-Abidin Saleh, International Legal Protection of Personal Data on the Internet between Conventional International Law and National Law, 1st ed., Arab Center for Studies, Publishing and Distribution, Cairo, Egypt, 2016, pp. 402–403.
[4] Seham Qaroun, op. cit., p. 1018.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

framework of an electronic commerce contract, only data that are relevant and necessary for the particular electronic commercial transaction may be collected. Such data must not be excessive, but rather accurate, complete, and limited to what is strictly required, while being updated whenever necessary.

Furthermore, personal data may not be retained for longer than necessary. They should only be kept for the period required to achieve the purposes for which they were collected and processed.

Conversely, once the purpose for which the personal data were collected has expired or been fulfilled, such data must be destroyed.[1]Consequently, personal data cannot lawfully constitute part of the commercial assets of an electronic supplier. Nevertheless, an electronic supplier may be tempted to treat customers' personal data as part of its business assets and sell them to other commercial websites, considering them an element of its business capital that may be marketed if necessary, for example in the event of bankruptcy. Such conduct, however, is prohibited by law and constitutes an infringement of the right to privacy. Moreover, it is often difficult to detect, since the seller may simply claim that the data were stolen from its information system.[2]

In addition, personal data may be used to implement discriminatory pricing policies, whereby products are offered at higher prices to customers considered to be wealthier.[3]

Second Requirement: Legal Controls for the Protection of Personal Information in Electronic Commerce Contracts

Article 26 of the Electronic Commerce Law imposes obligations on the electronic supplier within the framework of collecting personal data for the conclusion of electronic commercial transactions. These data mainly take the form of customer and prospective customer files. In addition to the previously mentioned conditions, the law requires compliance with a number of mandatory legal safeguards, the most significant of which are as follows:

Obligation to Ensure Information Security and the Confidentiality of Data in Electronic Commerce Contracts

Information security is regarded as one of the most fundamental requirements for the success of electronic commerce, as it strengthens trust among the parties involved. The essential components of such trust include, first, information security, namely the protection of exchanged information and the preservation of the integrity of electronic communications; second, privacy, which guarantees the confidentiality of customer transactions and assures customers that their online activities are not subject to unauthorized monitoring; and third, the reliability and authenticity of transaction requests, ensuring that the requests exchanged are genuine and correspond to those actually intended by the contracting parties.[4]

---

[1] Bader aldin daoudi, Protection of Electronic Privacy under Moroccan Legislation, Electronic Journal of Legal Research, Morocco, No. 3, 2019, p. 51.

[2] Flavien Serge Manionana, Vie privée en commerce électronique, PhD Thesis in Computer Science, Faculty of Graduate Studies, Université de Montréal, December 2005, p. 99.

[3] Ibid., p. 100.

[4] Nassar Mohammed Al-Halalmeh, Electronic Commerce in Law, 1st ed., Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2012, p. 172.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

In addition, information security requires the continuous availability of information and services by ensuring the uninterrupted functioning of information systems, maintaining the ability to interact with information, and guaranteeing that users are not prevented from accessing or using such information.[1]

Moreover, ensuring the integrity and confidentiality of personal data processing requires advanced electronic technical measures. Data security does not merely involve preventing unauthorized persons from accessing personal information; it also extends to protecting such data against threats to their existence, such as destruction or loss. Accordingly, electronic suppliers are required to adopt appropriate security measures, including the use of password-protected databases and the encryption of personal data during transmission through computer networks or the Internet. These measures constitute essential factors in strengthening and promoting the information society. In this regard, the Algerian legislator has required electronic suppliers to guarantee the security of information systems and the confidentiality of consumers' personal data by adopting all necessary technical and organizational safeguards.

Prohibition of Direct Electronic Prospecting

Electronic suppliers often rely on advertising techniques that may exert considerable psychological influence on electronic consumers, encouraging them to purchase goods or services that they do not actually need. Such techniques generally involve identifying and analyzing consumers' preferences and inclinations. To protect electronic consumers, the Algerian legislator has prohibited electronic suppliers from engaging in direct prospecting activities except in accordance with legally prescribed conditions.

It should be noted that the Arabic version of Article 31 uses the expression "prohibits direct surveying (al-istibyān)," whereas the French version employs the term "La Prospection Directe," meaning direct prospecting. This concept was expressly defined by the legislator in Article 3, paragraph 19, of Law No. 18-07, which also establishes the legal conditions governing its practice. Therefore, the term direct prospecting is the appropriate legal expression to be adopted when analyzing the provisions of Article 31 of the Electronic Commerce Law.

Definition of Direct Prospecting

Article 3, paragraph 19 of Law No. 18-07 defines direct prospecting as the sending of any message, regardless of its medium or nature, intended to directly or indirectly promote goods, services, or the reputation of a person selling goods or providing services.[2] This is essentially the same definition adopted by the Moroccan legislator, although the latter uses the term direct canvassing. The Tunisian legislator, on the other hand, refers to it as marketing and advertising. Accordingly, direct prospecting consists of the communications usually carried out by an enterprise with prospective consumers in order to persuade them and introduce them to the

[1] Adman Merizik & Bouglachi Imad, Information Security in the Context of Electronic Commerce: With Reference to the Cases of Tunisia and Algeria, New Economy Journal, University of Khemis Miliana, Vol. 2, No. 3, May 2011, p. 11.

[2] Article 3 of Law No. 18-07, previously cited.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

goods and services offered on the market, encouraging them to purchase such goods or services through messages regardless of their form or medium.[1]

The French legislator has also regulated and restricted direct prospecting. Pursuant to Article 22 of the Law of 21 June 2004, a new provision (Article L34-5) was introduced into the Postal and Electronic Communications Code, establishing the principle that any form of direct prospecting directed at natural persons is prohibited without their prior consent. Such consent must be expressed freely, explicitly, and unambiguously as an informed manifestation of will; otherwise, the offender is liable to criminal sanctions.[2]

Direct prospecting also aims to obtain a response or complete a commercial transaction, as it constitutes a form of electronic advertising. It relies on information and communication technologies to enable businesses to communicate with their customers by measuring customer responses and reactions through modern technological tools. It further benefits from the interactive nature of these technologies, which allows consumers to express their needs and preferences regarding the products they wish to obtain and the specifications they expect.[3]

Rules Governing Direct Prospecting

Legislators have sought to establish substantive and procedural legal rules governing direct prospecting in order to prevent infringements of informational privacy, particularly concerning personal data processed within the framework of electronic commercial transactions. The Algerian legislator addressed this issue through the provisions of Law No. 18-07 on the Protection of Natural Persons with regard to the Processing of Personal Data, as well as Chapter VII of the Electronic Commerce Law, entitled Electronic Advertising.

Obtaining the Explicit Consent of the Electronic Consumer

Pursuant to Article 7 of Law No. 18-07, the legislator expressly and unequivocally provides that personal data may not be processed without the explicit consent of the data subject. This principle is reaffirmed in Article 31 of the Electronic Commerce Law, which requires prior consent before sending direct solicitations through electronic communications. It also prohibits the use of a natural person's information in any manner inconsistent with Article 37(1) of Law No. 18-07, which prohibits direct prospecting by means of electronic communication systems, facsimile devices, e-mail, or any similar technological means using a natural person's personal data unless that person has given prior consent.[4]

The Electronic Consumer's Right to Object to Direct Prospecting

The legislator grants the electronic consumer the right to be informed, imposing an obligation on the entity conducting the prospecting operation to provide the necessary information, thereby

[1] Ben Said Sabrina & Nouiri Samia, "The Impact of Prohibiting Direct Prospecting on the Privacy of the Electronic Consumer," Annals of the University of Algiers 1, Vol. 35, No. 1, 2011, p. 323.

[2] Jean-Marc Décaudin & Jacques Digout, E-publicité: Les fondamentaux, Collection Management SUP, Dunod, Paris, 2011, p. 226.

[3] Mariam Yaghlab, "Direct Prospecting between Legitimacy and the Violation of the Right to Digital Privacy," Journal of Judicial Ijtihad, Faculty of Law and Political Science, University of Biskra, No. 12, October 2019, p. 123.

[4] Article 37(1) of Law No. 17-08, previously cited.

enabling the consumer to exercise the right to object. Article 32 of Law No. 18-07 stipulates that any person contacted for the purpose of collecting personal data must first be informed in advance, explicitly, and unambiguously. Consequently, the electronic consumer must be provided with sufficient information regarding the prospecting operation in order to express, with complete transparency and clarity, whether to object to or accept such communications.

For this purpose, Article 32 of the Electronic Commerce Law requires electronic suppliers to establish an electronic system enabling any individual to express, free of charge and without justification, their wish not to receive any further electronic advertising communications.

As a legal mechanism for protecting the electronic consumer, the electronic supplier is further required to issue an electronic acknowledgment confirming that the individual's request has been registered, pursuant to Article 32, paragraph 2, of the aforementioned law. This acknowledgment prevents the supplier from denying its obligations arising from this procedure and serves as proof that it has been notified of the consumer's request. It also facilitates the establishment of civil or criminal liability, where appropriate.

The legislator has also imposed a very short time limit within which the electronic supplier must comply with the electronic consumer's request. It is noteworthy, however, that the legislator did not specify the exact commencement of the 24-hour period. By reference to the general legal rules, this period should begin from the date of the final procedural act, namely the issuance of the acknowledgment of receipt, which constitutes evidence of notification for both the electronic consumer and the electronic supplier. Accordingly, the time limit becomes binding upon both parties.

Where a dispute arises concerning the supplier's compliance with the requirements laid down in Articles 30, 31, and 32 of the Electronic Commerce Law, the burden of proof rests upon the electronic supplier. The supplier must demonstrate compliance with both the substantive legal requirements and the relevant technical procedural obligations, including the establishment of an electronic system comprising the necessary technical means, namely a software program specifically designed for this purpose. Such software is defined as...

A set of instructions that sends commands to a device for execution. It should be noted that the program issues these commands based on the user's instructions.

A program is nothing more than a highly detailed set of instructions directed to a computer to execute whatever the programmer intends. Therefore, the computer can perform the tasks for which the program was designed.[1]

The OPT-OUT system, also referred to as the refusal or objection list system, is based on the principle that an advertiser may send commercial advertisements to consumers via email without obtaining their prior consent. If the consumer no longer wishes to receive such commercial advertisements, they must notify the advertiser of this preference. Once such notification is made, the advertiser is obliged to respect the consumer's request; otherwise, they incur legal liability. Under this system, sending commercial advertisements before the

[1] Rasha Ali Al-Din, The Legal System for the Protection of Software, Dar Al-Jami'a Al-Jadida, Alexandria, Egypt, 2007, pp. 12–13.

consumer objects is lawful, whereas sending them after the consumer has objected becomes unlawful. In practice, the OPT-OUT system is generally represented by a statement such as: "I agree to the use of my personal data for direct marketing or commercial advertising purposes." This statement appears on the consumer's webpage or screen, accompanied by two options at the bottom: Agree and Disagree, allowing the consumer to express their preference.[1]

Chapter Two: Technical Mechanisms for the Protection of Personal Data in Electronic Commerce Contracts for the Electronic Consumer

Section One: Electronic Signature and Electronic Certification as Mechanisms for Protecting Personal Data in Electronic Commerce Contracts

Electronic signatures and electronic certification constitute fundamental pillars and essential requirements for establishing trust and credibility in electronic commerce. They play a vital role in building confidence between contracting parties. In order to create a suitable electronic environment, the concept of the electronic signature emerged as a modern alternative to the traditional handwritten signature, which is no longer compatible with transactions conducted through advanced electronic communication technologies. Consequently, it became necessary to develop legislation governing the use of this technology and to provide a comprehensive legal framework for its regulation. Both international and national legislations have recognized this necessity. In line with these developments, the Algerian legislature enacted Law No. 15-04 concerning electronic signatures and electronic certification, which establishes the general rules governing electronic signatures and electronic certification services.[2]

Definition of the Electronic Signature

Legislators have attempted to clarify the meaning and concept of the electronic signature from different perspectives. Some definitions focus on the technological means by which the signature is created, while others emphasize the functions performed by the electronic signature. Accordingly, both doctrinal and legislative definitions are presented below.

1. Doctrinal Definition of the Electronic Signature

According to legal scholars, an electronic signature is any signature created by non-traditional means, namely through electronic methods or by using coordinated cryptographic algorithms processed by a computer system, resulting in a distinctive form identifying the owner of the signature. Others define it as letters, numbers, symbols, signs, sounds, or other electronic elements affixed to an electronic document that possess a distinctive character enabling the identification of the signer and expressing their consent to the legal transaction associated with the signature.[3]

---

[1] Khmikham Mohamed, Criminal Protection of the Electronic Consumer in Electronic Commerce Contracts: A Comparative Study, PhD Dissertation, Faculty of Law and Political Science, Abu Bakr Belkaid University, Tlemcen, 2017–2018, p. 91.

[2] Law No. 15-04 Establishing the General Rules Governing Electronic Signature and Electronic Certification, issued on 1 February 2015, Official Gazette No. 6, published on 10 February 2015.

[3] Abeer Mikhail Al-Safadi Al-Tawal, Electronic Signature, 1st ed., Dar Wael for Publishing and Distribution, Amman, Jordan, 2010, pp. 43–44.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 2,* 2026
Website: https://ceapress.org

Another scholarly definition describes the electronic signature as a set of technical procedures that make it possible to identify the person who generated those procedures and confirm their acceptance of the content of the document to which the signature relates.[1]

2. Legislative Definition of the Electronic Signature

At its thirty-fourth session, the United Nations Commission on International Trade Law (UNCITRAL) adopted the UNCITRAL Model Law on Electronic Signatures (2001). Article 1 provides that the Model Law applies whenever electronic signatures are used in the context of commercial activities. Article 2 defines an electronic signature as:

"Data in electronic form contained in, affixed to, or logically associated with a data message, which may be used to identify the signatory in relation to the data message and to indicate the signatory's approval of the information contained therein."[2]

Similarly, the Algerian legislature, in Chapter Two of Law No. 15-04, provides several definitions of the terms used in the Law. Article 2 defines the electronic signature as:

"Data in electronic form attached to or logically associated with other electronic data and used as a means of authentication."[3]

Forms of Electronic Signatures and Their Main Applications in Electronic Commerce.

Electronic signatures have countless applications due to their continuous evolution and daily development.[4] Electronic signatures take various forms and are legitimately and systematically used in the field of e-commerce to ensure security and provide a safe environment for conducting electronic transactions. An electronic signature may take the form of a digital signature, a biometric signature, a signature created using an electronic pen, or even a magnetic card combined with a personal identification number (PIN). The most important forms include the following:

1. Electronic Pen Signature

An electronic pen signature consists of transferring a handwritten signature by scanning it using a scanner, then inserting the scanned image into the electronic document to which the signature is to be attached in order to provide it with legal evidentiary value. Through this method, the signatory's handwritten signature is transmitted via electronic communication networks. This technique offers undeniable advantages due to its flexibility and ease of use, as it converts the traditional handwritten signature into an electronic format through information processing systems.[5]

---

[1] Issa Ghassan Rabadi, Special Rules Governing Electronic Signatures, 2nd ed., Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2012, p. 56.

[2] Saadi Al-Rubaie, The Evidentiary Value of the Electronic Signature under Algerian Legislation, PhD Dissertation, Faculty of Law and Political Science, University of Batna, 2015–2016, p. 40.

[3] Article 2(2) of Law No. 15-04, previously cited.

[4] Mohammed Fawaz Al-Mutalaqah, Electronic Commerce: A Comparative Study, 3rd ed., Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2011, p. 179.

[5] Tharwa Abdel Hamid, Electronic Signature: Its Nature, Risks, Means of Confronting Them, and Its Evidentiary Value, Dar Al-Jami'a Al-Jadida, Alexandria, Egypt, 2007, p. 55.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

2. Biometric Signature

The biometric signature represents a modern and advanced scientific method based on the unique biological and physiological characteristics of individuals. These characteristics include fingerprints, retinal scans, iris recognition, voice patterns and tone, hand geometry, facial recognition, and personal handwriting characteristics.

This application belongs to the field of biometrics, which relies on the digital measurement of the unique characteristics of human beings to distinguish one individual from another.[1] Consequently, the biometric signature is regarded as a highly reliable means of authentication.[2]

3. Digital Signature

The digital signature is one of the principal forms of electronic signatures used to conclude legal transactions through electronic means over the Internet. It relies on cryptographic techniques (La Cryptographie), which, from a technical perspective, constitute a branch of applied mathematics concerned with transforming plain, readable text into encrypted text through complex mathematical equations known as encryption algorithms.[3]

This method requires the use of two cryptographic keys: a public key and a private key. Through the public key, any person may read the transmitted message or data available over the Internet, but no one can modify it unless they possess the corresponding private key.[4] The Algerian legislator, under Article 2, Paragraph 8 of Law No. 15-04, defines the private key as a sequence of numbers exclusively possessed by the signatory and used to create the electronic signature. This private key is associated with a corresponding encryption key.[5]

Likewise, the Algerian legislator defines the public key in Article 2, Paragraph 9 of Law No. 15-04 as a sequence of numbers made available to the public for the purpose of verifying the electronic signature and included in the electronic certification certificate.

The digital signature has a remarkable capacity to accurately identify the parties involved and enjoys a high degree of reliability in the conclusion of contracts, making it one of the most significant forms of electronic signatures.[6]

Third: The Importance of Electronic Signatures in Protecting Personal Data in Electronic Commerce Contracts

Electronic signatures contribute significantly to the expansion of electronic commerce by securing electronic transactions and preserving the confidentiality of communications and exchanges. They prevent unauthorized persons from accessing, modifying, or altering the content of electronic communications. Moreover, electronic signatures grant legal evidentiary value to documents generated through the Internet and are recognized before courts of law, thereby facilitating effective judicial oversight of electronic commerce.

---

[1] Abeer Mikhail Al-Sadafi Al-Toul, Previous Reference, p. 51.
[2] Tharwat Abdel Hamid, Previous Reference, p. 61.
[3] Saadi Al-Rabee, Previous Reference, p. 57.
[4] Fadi Mohammed Imad Tawakkul, Previous Reference, p. 160.
[5] Article 2, Paragraph 8 of Law No. 15-04, Previous Reference.
[6] Shadi Ibrahim, Previous Reference, p. 311.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

Furthermore, electronic signatures enable the electronic identification of both the sender and the recipient, verify the identity of the parties and the authenticity of the transmitted information, and enhance the levels of security and privacy for participants engaged in electronic commerce.[1] They accurately identify the person who performed the signature and confirm the authenticity and integrity of the associated data and content.

In addition, electronic signatures strengthen trust between the parties to electronic commercial contracts by ensuring security and reliability. They facilitate the rapid conclusion of contracts, promote the expansion and development of electronic commerce, contribute to its legal stability, and provide legal protection in light of its continuous and accelerating growth.

The Algerian legislator, pursuant to Article 12 of the Electronic Commerce Law, requires that, at the final stage of concluding an electronic commercial contract, the electronic consumer must confirm their acceptance by electronically signing the contract, in order to ensure the protection of personal data.

Section Two: Electronic Certification as a Mechanism for the Protection of Personal Data in Electronic Commerce Contracts

The numerous advantages of electronic transactions and the continuous growth in their volume—particularly within the field of electronic commerce—have naturally resulted in numerous disputes, compelling states to seek effective and scientific solutions capable of adapting to the evolution of electronic transactions while fostering trust, confidence, and security among users. Consequently, an extremely important system emerged out of this pressing need: the electronic certification system. It constitutes the backbone of electronic transactions by granting authenticated electronic transactions legal value and evidentiary force equivalent to that of traditional transactions. Electronic certification authenticates electronic transactions, attributes them to their rightful originators, and prevents alteration or manipulation through a neutral third party,[2] whether a public or private entity, that issues electronic certificates. Legislations differ in terminology according to their legal systems, using expressions such as electronic certification service provider or electronic authentication service provider.

First: Definition of Electronic Certification

Electronic certification or electronic authentication is a secure technical mechanism used to verify the authenticity of an electronic document or record by confirming that it originates from a specific individual through a neutral entity known as the electronic certification (or authentication) service provider.

It is also defined as the process of verifying that an electronic signature has been created by a specific person through the use of analytical techniques designed to identify symbols, words,

[1] Barakat Karima, The Legal Regulation of Electronic Signatures as a Mechanism for the Development of Electronic Commerce in Algeria, in the Research Series on Consumer Protection in Electronic Commercial Transactions, Publications of the Laboratory of Digitalization and Law in Algeria, Faculty of Law and Political Science, University of Blida 2, 2020, pp. 337–338.

[2] Akram Tahsin Al-Dukhaili, The Legal Framework of Electronic Certification: A Comparative Study, 1st ed., Zain Legal Publications, Beirut, Lebanon, 2018, p. 12.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

numbers, decryption methods, reverse engineering techniques, or any other means or procedures capable of achieving the intended verification purpose.[1]

Within Arab legislations, the Omani Electronic Transactions Law No. 69/2008, issued on 17 May 2008, defines electronic certification procedures as procedures intended to verify that an electronic message has originated from a specific person and to detect any error or alteration in the contents, transmission, or storage of an electronic message or electronic record during a specified period. Such procedures include any process employing mathematical algorithms, symbols, words, identification numbers, encryption, acknowledgment or receipt procedures, or any similar information security techniques.[2]

As for the Algerian legislator, a definition of electronic certification was introduced in the Official Gazette of Parliamentary Debates relating to Law No. 15-04, where the rapporteur of the Transport and Telecommunications Committee, while presenting the preliminary report before the members of the National People's Assembly, stated that electronic certification may be defined as the procedures through which confidence is established in the identity of users of information systems by automated means.[3]

Furthermore, pursuant to Article 28 of the Electronic Commerce Law, the legislator requires every electronic supplier to connect its website to a secure electronic payment platform protected by an electronic certification system.[4]

Third: The Importance of Electronic Certification in Protecting Personal Data within Electronic Commerce Contracts

1. Verifying the Identity of the Contracting Party

Electronic certification enables the definitive verification of the identity of the person who issued the electronic data, whether a natural or legal person, as well as confirming the legal capacity of the contracting parties and the content of the contract. Article 42(2) of Law No. 15-04 stipulates that an electronic certification service provider may issue an electronic certificate only after verifying the applicant's identity and, where appropriate, verifying their specific legal attributes.[5] Confirming that the electronic signature genuinely belongs to its owner constitutes a fundamental safeguard for personal data in electronic commerce contracts.

2. Ensuring the Integrity and Confidentiality of Exchanged Data

The certification authority is responsible for proving the existence, content, and integrity of electronic exchanges between contracting parties while ensuring that such exchanges are free from fraud and manipulation. To prevent fraudulent activities directed against users,

[1] Fatima Al-Zahra Mossaddaq, "Electronic Certification as a Means of Protecting Electronic Signatures," Journal of Legal Studies and Research, Faculty of Law and Political Science, Mohamed Boudiaf University, M'Sila, Vol. 5, No. 1, May 2020, p. 38.

[2] Dahmani Samir, Previously Cited Reference, p. 33.

[3] National People's Assembly, Official Gazette of Parliamentary Debates, Previous Legislative Term, Fifth Ordinary Session, Public Sitting held on 25 November 2014.

[4] Article 28 of Law No. 18-05, previously cited.

[5] Article 42 of Law No. 15-04, previously cited.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

certification authorities monitor commercial websites by verifying their actual existence and credibility.[1]

Moreover, Article 40 of Law No. 15-04 obliges certification service providers to preserve the confidentiality of all information and data relating to the electronic certificates they issue.

3. Determining the Time of Contract Formation

Although determining the exact time of contract formation is not a condition for the validity of the contract, it marks the commencement of the legal effects arising from it. Since users can alter the time settings on their computers, and because determining the time of contract formation becomes increasingly complex when the contracting parties are located in different countries using computer systems operating on different time settings, the determination of the official time of contract formation should be carried out through certification authorities, which establish a single official timestamp for the conclusion of the electronic contract.[2] Accordingly, the electronic certification process accurately determines the precise moment at which electronic messages are exchanged and received.

5. Ensuring the Non-Repudiation of Data Messages Issued by Either Party[3]

Certification authorities act as neutral third parties by issuing digital certificates that authenticate electronic signatures and guarantee their non-repudiation. In other words, neither the sender nor the recipient can evade their contractual obligations by denying the signature or disputing any of the data contained therein. This is because the data message can only be accessed by the intended recipient through the use of their private encryption key.

Section Two: Technical Security of Electronic Payment Methods as a Mechanism for Protecting Personal Data

Since electronic payment transactions are conducted between the electronic consumer and the electronic supplier, the data exchanged during such transactions can easily be copied, altered, or tampered with. To avoid the risks arising from such practices, it is essential to establish a secure payment system. Security may be achieved through technical as well as legal means. In reality, payment security is effective only when technical and legal safeguards complement and reinforce one another. Likewise, an integrated payment security system must ensure that the payment process is protected against any external intrusions.[4]

One of the principal technical methods used to secure electronic payment systems is cryptography, or the science of transforming data messages into coded symbols and numerical sequences so that they become unintelligible to unauthorized persons. This technology is used confidentially over the Internet and aims to preserve data confidentiality through encryption

[1] Article 63, ibid.

[2] Koussam Amina, Previously Cited Reference, p. 6.

[3] Shabi Adham Tantawi, The Legal Framework of Contracting and Electronic Signatures in Electronic Commerce Contracts, 1st ed., Arab Studies Center, Arab Republic of Egypt, 2016, p. 326.

[4] Marouf Mustafa Abbas Al-Shafie, The Legal Framework of Electronic Payment and Settlement Methods: A Comparative Study, Ph.D. Dissertation, Faculty of Graduate Studies, Omdurman Islamic University, Sudan, 2011, p. 406.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 2,* 2026
Website: https://ceapress.org

algorithms employing cryptographic keys or passwords that are available only to authorized users.[1]
Encryption algorithms are complex mathematical procedures used to encrypt and decrypt data in order to ensure the confidentiality required for protecting information. Their purpose is to secure transactions conducted among the online customer, the merchant, and the bank by restricting access to and reading of the information solely to the legitimate parties involved in the transaction.[2]
The Algerian legislator, pursuant to the provisions of Law No. 15-04 establishing the general rules governing electronic signatures and electronic certification, defined encryption keys in Article 2, paragraphs (8) and (9), under the section entitled "Definitions." It defines the private encryption key as a sequence of numbers possessed exclusively by the signatory and used to create the electronic signature, which is linked to a corresponding public key. The law further defines the public encryption key, in paragraph (9) of Article 2, as a sequence of numbers made available to the public for the purpose of verifying the electronic signature and incorporated into the electronic certification certificate.[3]
Another modern security mechanism is the use of firewalls (FIREWALLS). This technology has been widely adopted by companies operating in the fields of information technology and network security to protect networks and prevent suspicious Internet connections from gaining unauthorized access to internal systems.[4]
A firewall operates by filtering data transmitted across the network. It serves as an intermediary between a personal computer and the Internet, processing and analyzing all data and information exchanged between domestic and international users through the network.[5]
Accordingly, the Algerian legislator requires electronic service providers to secure electronic payment data and subjects electronic banking operations to the supervision of the Bank of Algeria in order to ensure the confidentiality, integrity, and security of the exchanged data.

01- Security through the Electronic Certification System

Pursuant to Article 28 of the Electronic Commerce Law, the Algerian legislator has made it mandatory to secure electronic payment platforms through an electronic certification system. Given the particular nature of electronic banking transactions compared with other electronic commercial transactions, and the necessity of identifying and verifying the customer's identity before completing payment, the first application of electronic authentication within the electronic commerce system emerged in the field of electronic payment systems. Customer

[1] Noufla Saylah, op. cit., p. 218.
[2] Youssef Waqed, The Legal Framework of Electronic Payment, Master's Thesis, Faculty of Law, Mouloud Mammeri University, Tizi Ouzou, 2011, p. 162.
[3] Article 2, paragraphs (8) and (9) of Law No. 15-04, op. cit.
[4] Abdel Rahim Wahiba, The Replacement of Traditional Banking Payment Instruments with Electronic Means of Payment: The Case of Algeria, Master's Thesis, Faculty of Economics and Management Sciences, University of Algiers, 2008, p. 34.
[5] Waqed Youssef, Previously Cited Reference, p. 170.

identity is verified when using a bank card, whereby the parties to the card transaction agree upon one of the recognized forms of electronic authentication.[1]

In the context of electronic payment methods, electronic certification refers to the authentication of messages exchanged between the bank and the customer that contain data and information related to transactions carried out through electronic payment instruments. Certifying such data means verifying that the payment order has indeed been issued by the person to whom it is attributed by confirming that person's identity and ensuring that no alteration or modification has occurred in the electronically exchanged document.[2] Thus, while the electronic signature serves as a means of verifying a person's identity and expressing his or her consent and approval of the transaction, verification of the electronic signature also confirms its integrity during the payment process.

Verification of the electronic signature of the account holder during payment ensures the validity and integrity of the signature, contributes to the secure and successful completion of bank transfers, and confers official legal status upon the payment transaction through the electronic certificate, which constitutes a guarantee of trust between the parties to the transaction. Comparative legislation in several Western countries has authorized banks to provide certification services in order to strengthen customer confidence, although certification services were traditionally entrusted to independent authorities or institutions—commonly referred to as trusted third parties—to ensure public trust. In France, the French Central Bank became the first central bank to be recognized as an electronic certification service provider in accordance with the European standard ETSI/TS 101 456 and pursuant to the Decree of 26 July 2004 establishing the conditions for the acceptance of electronic signatures approved by the Ministry of Economy, Finance and Industry.[3] It would be desirable for the Algerian legislator to follow a similar approach.

02- Subjecting the Electronic Payment System to the Supervision of the Bank of Algeria

Banking is one of the most vital economic activities due to its close relationship with overall economic activity. Consequently, modern legislation in various countries has attached great importance to regulating, supervising, and monitoring the banking sector through the establishment of specialized supervisory bodies.[4] The expansion of electronic commerce has led to the emergence of modern payment methods, transforming traditional banking activities into electronic systems that require regulatory oversight. Accordingly, Article 29 of the Electronic Commerce Law subjects electronic payment platforms to the supervision of the Bank of Algeria to ensure interoperability requirements and to guarantee the security and reliability of payment operations.

---

[1] Saber Mohamed Mahmoud Al-Maz'al, "Electronic Authentication in Banking Transactions: A Comparative Study," Legal Journal, Cairo University, Faculty of Law (Khartoum Branch), Egypt, Vol. 2, No. 2, 2017, p. 230.

[2] Ghazali Naziha, "Legal Mechanisms for the Protection of Electronic Payment Instruments," Journal of Political and Administrative Research, University of Djelfa, No. 10, June 2017, p. 291.

[3] Slih Bounafla, Previously Cited Reference, p. 387.

[4] Marwa Bougadoum & Djamel Amoura, "Banking Supervision in Algeria and Its Role in Enhancing Disclosure in Algerian Banks," Journal of Economic Research, University of Blida 2, No. 18, June 2018, p. 68.

In its practical sense, banking supervision refers to activities aimed at minimizing the likelihood of errors and deviations to the lowest possible level, even though such risks cannot be entirely eliminated.[1] Under Chapter Four of Law No. 23-09 concerning Monetary and Banking Law, entitled "Security of Payment Systems," particularly Articles 58 and 59, the Bank of Algeria has been entrusted with responsibility for ensuring the sound functioning of payment systems.
Article 58 provides that the Bank of Algeria shall ensure the proper functioning, efficiency, and security of all national payment systems under its authority.[2] It also verifies the safety of payment instruments and their compliance with the applicable standards. The Bank may refuse the introduction of any payment instrument that does not provide adequate safeguards or may require corrective measures where the payment instrument is incompatible with the existing technical infrastructure.

Furthermore, Article 59 of the same Law stipulates that the Bank of Algeria shall verify the security of payment instruments other than credit currency, regardless of the issuing institution. It is also responsible for establishing and updating the standards applicable in this field and for creating a Standardization Committee to oversee their implementation.[3]

Article 4 of Regulation No. 05-07 concerning the Security of Payment Systems stipulates that the security of payment systems encompasses the security of the payment systems infrastructure as well as the payment instruments that are legally in force pursuant to the provisions of Article 166 of Law No. 23-09, which repealed all provisions inconsistent with this Law, particularly those contained in Law No. 03-11 on Money and Credit. However, the implementing regulations issued under the repealed law shall remain in force until the promulgation of the implementing texts adopted pursuant to this Law.[4]

2. Supervision to Preserve the Confidentiality, Integrity, and Security of Exchanged Data

Article 29 of the Electronic Commerce Law requires the preservation of data confidentiality and customer privacy. Among the most important obligations imposed on banks is the protection of confidential information in order to ensure the continuity and sustainability of banking operations. Since electronic banking transactions are conducted through electronic platforms, particularly the Internet, confidentiality risks involve serious security dimensions that necessitate the provision of robust protection software to address such risks.

These risks are not confined solely to the technical responsibilities of banks; they also have significant legal implications. Consequently, strict legislation is required to oblige banks, customers, and electronic service providers to safeguard the confidentiality of the data to which they have access. Furthermore, competent supervisory authorities must exercise stringent oversight to ensure the highest possible level of protection against breaches of confidentiality.[5]

[1] Jalailia Abdeljalil, Mechanisms for Activating Banking Supervision over Electronic Banking: The Case of Algeria, Ph.D. Dissertation, Faculty of Economics, Ahmed Draia University, Adrar, 26 January 2020, p. 34.
[2] Article 58 of Law No. 23-09, Previously Cited Reference.
[3] Article 59 of Law No. 23-09, Previously Cited Reference.
[4] Article 4 of Regulation No. 05-07 concerning the Security of Payment Systems, dated 28 December 2005, Official Gazette No. 37, issued on 4 July 2006.
[5] Ziyad Tariq Jasim Al-Rai & Mohammed Ibrahim Abdullah, Previously cited, p. 48.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 *Issue 2,* 2026
Website: https://ceapress.org

Accordingly, banks are committed to implementing the highest international standards and adopting best practices in the field of information security, both with respect to their internal information systems and to systems containing customer information. For example, banks reinforce their information systems against potential cyberattacks by implementing multiple layers and levels of protection rather than relying on a single security mechanism[1].
Banking confidentiality constitutes a legal obligation incumbent upon the bank toward every person or entity dealing with it, even if only once. This obligation requires the bank not to disclose any information relating to a fact or banking transaction carried out by the customer, even where disclosure is requested by that customer, except in accordance with the applicable legal framework. The legal criteria governing banking confidentiality determine which information and facts must remain confidential, namely those obtained through banking activities, provided that such banking facts are not publicly known and constitute legally recognized facts.[2]
Preserving the confidentiality of data and ensuring the security of its exchange serve to protect all parties involved in electronic banking transactions, including electronic service providers and electronic consumers, as well as the public interest in every country. Banking confidentiality fosters trust and confidence among individuals and holders of financial assets.
...in a manner that guarantees the confidentiality of their banking operations and all related information, thereby creating an atmosphere of trust and fair competition, which ultimately contributes to the overall growth and prosperity of the national economy. [3]
The Algerian legislator has embodied this principle in Article 10 of Regulation No. 05-07 on the Security of Payment Systems, which provides that: "Participants in payment systems shall ensure the confidentiality and integrity of the information transmitted through payment systems." [4]This constitutes an obligation aimed at protecting the parties involved in banking transactions, strengthening confidence in the use of payment systems, and safeguarding the security of financial operations. Likewise, Law No. 23-09 on Monetary and Banking Law, in Article 133, emphasizes strict compliance with banking secrecy, subject to the penalties prescribed under the Penal Code. [5]
Conclusion
The Algerian legislator has attached great importance to the protection of personal data through the enactment of Law No. 18-07 of 10 July 2018, as amended and supplemented by Law No. 25-11 of 24 July 2025, which establishes the legal framework and institutional mechanisms governing the protection of personal data. This framework complements the relevant

[1] Laajal Dhahabiya & Qasi Si Youcef, "The Status of Banking Confidentiality in Light of Banks' Reliance on Electronic Banking Services," Journal of Legal Studies, University of Moulay Tahar, Saida, Vol. 8, No. 2, November 2021, p. 47.
[2] Mohammed Ali Al-Sarmid, Legal Aspects of Banking Confidentiality: A Comparative Study, Master's Thesis, Faculty of Law, Al-Ibra Private University, Jordan, 25 February 2009, p. 8.
[3] Ibid., p. 11.
[4] Article 10 of Regulation No. 05-07, op. cit.
[5] Article 133 of Law No. 23-09, op. cit.

legislation, particularly Law No. 09-04 on the specific rules governing Information and Communication Technologies (ICT), Law No. 15-04 establishing the general rules relating to electronic signatures and electronic certification, and Law No. 18-04 establishing the general rules governing postal services and electronic communications. Together, these legislative instruments reinforce regulatory and protective mechanisms in harmony with international standards in this field.

Furthermore, the legislator has strengthened the protection of electronic consumers by safeguarding their personal data in commercial transactions through Law No. 18-05 on Electronic Commerce, which imposes a legal obligation upon the electronic supplier under Article 26 of the same law to comply with all applicable legal and regulatory provisions concerning the processing and protection of personal data.

Since electronic commerce contracts necessarily require the collection and processing of consumers' personal data, they also require the implementation of a comprehensive set of measures designed to preserve the confidentiality and privacy of such data. These safeguards are essential for establishing trust, transparency, and integrity in electronic commercial transactions.

References

A. Books

1-Ayman Mostafa Ahmed Al-Baqli, Protection of Informational Privacy in Light of the Requirements of Electronic Commerce, Legal Journal, Faculty of Law, University of Khartoum, No. 4, 2021.

2-Akram Tahsin Al-Dukhaili, The Legal Framework of Electronic Authentication: A Comparative Study, 1st ed., Zain Legal Publications, Beirut, Lebanon, 2018.

3-Ben Saïd Sabrina and Nouiri Samia, The Impact of the Prohibition of Direct Prospecting on the Privacy of the Electronic Consumer, Annals of the University of Algiers 1, Vol. 35, No. 1, 2011.

4-Ben Saïd Sabrina and Nouiri Samia, The Impact of the Prohibition of Direct Prospecting on the Privacy of the Electronic Consumer, Annals of the University of Algiers 1, Vol. 35, No. 1, 2011.

5-Barakat Karima, The Legal Regulation of Electronic Signatures as a Mechanism for the Development of Electronic Commerce in Algeria, in Research Series on the Protection of the Electronic Consumer in Commercial Transactions, Digitalization and Law Laboratory Publications, Faculty of Law and Political Science, University of Blida 2, 2020, pp. 337–338.

6-Rasha Ali Al-Din, The Legal Framework for Software Protection, New University Publishing House, Alexandria, Egypt, 2007.

7-Abeer Mikhael Al-Safadi Al-Tawal, Electronic Signature, 1st ed., Dar Wael for Publishing and Distribution, Amman, Jordan, 2010.

8-Issa Ghassan Rabadi, Special Rules Governing Electronic Signatures, 2nd ed., Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2012.

9-Tharwa Abdel Hamid, Electronic Signature: Its Nature, Risks, Methods of Addressing Them, and Its Evidentiary Value, New University Publishing House, Alexandria, Egypt, 2007.

10-Saber Mohamed Mahmoud Al-Mazal, Electronic Documentation in Banking Business: A Comparative Study, Legal Journal, Cairo University, Faculty of Law (Khartoum Branch), Egypt, Vol. 2, No. 2, 2017.
11-Shabi Adham Tantawi, The Legal Framework of Contracting and Electronic Signatures in Electronic Commerce Contracts, 1st ed., Arab Studies Center, Arab Republic of Egypt.
12-Marwa Zein El Abidine Saleh, International Legal Protection of Personal Data on the Internet between International Conventional Law and National Law, 1st ed., Arab Center for Publishing and Distribution, Cairo, Egypt, 2016.
13-Mohammed Fawaz Al-Mutalaqah, Electronic Commerce: A Comparative Study, 3rd ed., Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2011.
14-Nassar Mohammed Al-Halalmeh, Electronic Commerce in Law, 1st ed., Dar 15-Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2012.

B. Doctoral Dissertations and University Theses

B.1. Doctoral Dissertations

1-Khmeikhem Mohamed, Criminal Protection of the Electronic Consumer in Electronic Commerce Contracts: A Comparative Study, Ph.D. Dissertation, Faculty of Law and Political Science, Abou Bekr Belkaid University, Tlemcen, 2017–2018.
2-Saadi Rabie, The Evidentiary Value of Electronic Signatures in Algerian Legislation, Ph.D. Dissertation, Faculty of Law and Political Science, University of Batna, 2015–2016.
3-Marouf Mostafa Abbas Al-Shafie, The Legal Framework of Electronic Payment and Settlement Methods: A Comparative Study, Ph.D. Dissertation, Faculty of Graduate Studies.
4-Jelailia Abdeljalil, Mechanisms for Enhancing Banking Supervision over Electronic Banking: The Case of Algeria, Ph.D. Dissertation, Faculty of Economic Sciences, Ahmed Draia University, Adrar, 26 January 2020.

B.2. Master's Theses

1-Mohammed Ali Al-Sarmid, Legal Aspects of Banking Secrecy: A Comparative Study, Master's Thesis, Al-Ibra Private University, Faculty of Law, Jordan, 25 February 2009.
2-Ouaked Youcef, The Legal Framework of Electronic Payment, Master's Thesis, Faculty of Law, Mouloud Mammeri University, Tizi Ouzou, 2011.
3-Abdelrahim Ouahiba, The Replacement of Traditional Banking Payment Instruments by Electronic Means: The Case of Algeria, Master's Thesis, Faculty of Economic Sciences and Management Sciences, University of Algiers, 2008.
4-Mohammed Ali Al-Sarmid, Legal Aspects of Banking Secrecy: A Comparative Study, Master's Thesis, Al-Ibra Private University, Faculty of Law, Jordan, 25 February 2009.

D.1. Legislation

1-Law No. 16-01 concerning the Constitutional Amendment, dated 6 March 2016, Official Gazette No. 14, issued on 7 March 2016.
2-Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data, Official Gazette No. 34, issued on 10 June 2018.
3-Law No. 18-05 relating to Electronic Commerce, dated 10 May 2018, Official Gazette No. 28, issued on 16 May 2018.

Cadernos de Pós-Graduação em Direito Político e Econômico
Published by: Centro de Estudos Acadêmicos Press
ISSN: 1678-2127
Volume 26 ***Issue 2,*** **2026**
Website: https://ceapress.org

4-Law No. 15-04 establishing the General Rules Governing Electronic Signature and Electronic Certification, dated 1 February 2015, Official Gazette No. 6, issued on 10 February 2015.
5-Regulation No. 05-07 concerning the Security of Payment Systems, dated 28 December 2005, Official Gazette No. 37, issued on 4 July 2006.
6-People's National Assembly, Official Gazette of the Proceedings of the Previous Legislative Term, Fifth Ordinary Session, Public Sitting held on 25 November 2014.

Journals

1-Siham Qaroun, "The Obligation of the Electronic Supplier to Protect the Consumer's Personal Data under Law No. 18-05 on Electronic Commerce," Al-Bahith Journal for Academic Studies, Faculty of Law and Political Science, University of Hadj Lakhdar Batna 1, Vol. 7, No. 2, June 2020.
2-Badr Eddine Daoudi, "Protection of Electronic Privacy in Moroccan Legislation," Electronic Journal of Legal Research, Morocco, No. 3, 2019.
3-Admane Merizk and Bouglachi Imad, "Information Security in the Context of Electronic Commerce: With Reference to the Cases of Tunisia and Algeria," New Economy Journal, University of Khemis Miliana, Vol. 2, No. 3, May 2011.
4-Meriem Yaghlab, "Direct Prospecting between Legality and the Violation of the Right to Digital Privacy," Journal of Judicial Ijtihad, Faculty of Law and Political Science, University of Biskra, No. 12, October 2019.
5-Fatima Zahra Mosaddak, "Electronic Certification as a Means of Protecting the Electronic Signature," Journal of Legal Studies and Research, Faculty of Law and Political Science, Mohamed Boudiaf University of M'Sila, Vol. 5, No. 1, May 2020.
6-Ghazali Naziha, "Legal Mechanisms for the Protection of Electronic Payment Methods," Journal of Political and Administrative Research, University of Djelfa, No. 10, June 2017.
7-Marwa Bougadoum and Djamel Amoura, "Banking Supervision in Algeria and Its Role in Enhancing Disclosure in Algerian Banks," Journal of Economic Research, University of Blida 2, No. 18, June 2018.
8-Laâjal Dhahbia and Kassi Si Youcef, "The Status of Banking Secrecy in Light of Banks' Adoption of Electronic Banking Services," Journal of Legal Studies, University of Moulay Tahar Saida, Vol. 8, No. 2, November 2021.

Foreign-Language References

1-Flavien Serge Manionana, Privacy in Electronic Commerce. Ph.D. Dissertation in Computer Science, Faculty of Graduate Studies, Université de Montréal, December 2005.
2-Karim Seffar, The Regulation of Global Electronic Commerce. Doctoral Dissertation, Faculty of Graduate Studies, Université de Montréal, 2013.
3-Jean-Pierre Clavier and Alexandra Mendoza-Caminade, op. cit.
4-Jean-Marc Décaudin and Jacques Digout, E-Publicity: The Fundamentals, Management SUP Collection, Dunod Publishers, Paris, 2011.