European Journal of Philosophical Research. 2026. 13(1)
E-ISSN: 2413-7286
Volume-13/Issue-1/2026

The Law on Electronic Signature and Electronic Certification as One of the Guarantees for Preserving Public Order and Public Morals in the Digital Environment

Dr. Sahraoui Mustapha[1]
[1] University of Oran 2 Mohamed Ben Ahmed, Algeria.
E-mail: kmsahraoui@gmail.com

Submission: 27.06.2025| Acceptance: 15.03.2026| Publication: 03.06.2026

Abstract:
This research examines and analyzes one of the legal mechanisms adopted by the Algerian legislator to protect public order and public morals in the digital environment, through Law No. 15-04, which establishes the general rules governing electronic signature and electronic certification. The legislator has surrounded this significant instrument of electronic transactions with a set of legal safeguards. Among the provisions contained in the aforementioned Law No. 15/04 is the regulation of preventive measures based primarily on encryption as a mechanism for securing electronic signatures, alongside electronic certification, which guarantees the security requirements of information exchange over the Internet.
Keywords: Electronic signature, Electronic certification, Electronic-signature creation mechanism, Public order, Public morals, Digital space.

Introduction:

Despite the significant opportunities offered by Internet services in the field of electronic transactions and contract formation, they have also raised numerous legal challenges. Perhaps the most important of these is remote signing, namely signature via the Internet. Such issues require protection for exchanged data, that is, legal protection for transactions conducted through modern communication networks. This has required replacing traditional paper documents with non-paper supports, thereby creating broader openness to commercial exchange and economic relations between states. Consequently, presenting products, goods, and services, completing deals, and concluding contracts no longer require the contracting parties to travel or meet in a specific place. There is no doubt that concluding such contracts in electronic space is inevitably influenced by the need to protect public order and public morals, in order to confer upon them the character of a legal act that lacks a physical medium and is transformed into encrypted digital data known as the electronic signature. On the one hand, this has led to the emergence of a new concept of writing in electronic space, where electronic writing appeared in conjunction with the electronic signature. On the other hand, it required addressing these risks through the mechanisms of electronic signature and electronic certification.

For this reason, the Algerian legislator took the initiative to issue Law No. 15/04, which establishes the general rules governing electronic signature and electronic certification, with the aim of responding to the legal, regulatory, and technical requirements necessary to create an atmosphere of trust. This is intended to generalize and develop electronic exchanges and to establish the general principles governing electronic signature and electronic certification activities in Algeria. This legal framework also enables several sectors, including electronic administration and electronic commerce, to keep pace with digital transformation, thereby ensuring better management of bodies and institutions.

Among the provisions contained in the aforementioned Law No. 15/04 is the regulation of preventive measures based mainly on encryption as a means of securing the electronic signature, alongside the mechanism of electronic certification, which guarantees the security requirements of information exchange over the Internet, namely confidentiality, authentication, integrity, and non-repudiation. These aspects make it possible to establish a climate of trust for various electronic transactions, all of which contribute to preserving public order and public morals. This leads to the following problematic question: What role does Law No. 15-04 relating to electronic signature and electronic certification play in preserving public order and public morals during the conclusion of various electronic contracts?

To answer this problematic question, the study was structured into two sections. The first section addresses the meaning of public order and public morals and their relationship with the digital environment. The second section examines the concept of electronic signature and electronic certification, as well as the important role played by this legal text in preserving public order and public morals.

The First Section: The Meaning of Public Order and Public Morals and Their Relationship with the Digital Environment

Every community, regardless of its form of organization, requires a system of rules that regulates the conduct of individuals within it. These rules carry the authority to command and prohibit, accompanied by sanctions imposed on those who violate this system. They express the precedence of the higher public interest of the state and society over individual will and private interests.

The idea of public order, as expressed by Dr. Tarek El-Bishry, "constitutes an umbrella under whose legitimacy all legal acts must fall; otherwise, nullity shall be their sanction."[1]

Accordingly, this section focuses on identifying the legal origin of public order and public morals by clarifying the meaning of each and their relationship with the digital environment.

The First Requirement: The Concept of Public Order

A concept is, by nature, defined and precise, and requires a body of legal doctrine to support and develop it, as it represents the outcome of intellectual effort and conceptual reasoning. Legislative systems and positive jurisprudence have given considerable importance to public order, treating it

[1] Imad Tarek El-Bishry, same reference, p. 49.

as a central concept. However, its definition and limits remain, to this day, unclear and marked by a degree of ambiguity and indeterminacy.

This is because the legislator, when drafting legal provisions, may deliberately include certain flexible concepts such as rules of justice and equity, good faith, abuse of rights, and public order[2]. These notions are inherently indeterminate, yet they facilitate the application of legal rules. Resorting to them broadens the scope of interpretative authority, since ambiguity constitutes the very element that generates interpretation and forms the basis of legal reasoning.

By referring to the writings of jurists who have addressed the idea of public order, one observes a general consensus on the difficulty of providing a precise definition of this concept, as it remains, in essence, an elusive notion.

According to Counselor Pilon, the search for the concept of public order is similar to walking on shifting sands.[3]

Accordingly, clarifying the concept of public order requires, first and foremost, tracing the developments this concept has undergone in order to determine its meaning within Algerian law. Moreover, conceptual clarity can only be achieved by identifying the criteria and sources of public order.

First Branch: The Evolution of Public Order and the Determination of Its Concept in Algerian Law

The notion of public order is directly linked to society. On the one hand, it reflects the political, social, and economic foundations upon which society is built, expressed through legal rules endowed with a binding force that exceeds that of ordinary legal rules. On the other hand, it protects these foundations from any threats, whether internal or external.

The idea of public order, in both its emergence and development, is closely connected to the rise of the nation-state, that is, a politically organized society divided into rulers and the governed.

1- The Evolution of the Idea of Public Order:

A review of the various foundations upon which legal systems have been established, both historically and in modern times, reveals an essential fact: every community, regardless of its form of organization, has a constant need for a system of rules that regulates the conduct of individuals within it. These rules exercise authority through commands and prohibitions, always accompanied by sanctions imposed in cases of violation.[4]

This normative system, which restricts individual will in favor of societal necessities, is determined by the priorities of each community according to its philosophical, ethical, and religious references, as well as its political, economic, and social conditions and interests. Individual will therefore

---

[2] Alyan Ouda, *The Concept of Public Order and Freedom of Contract in Light of Algerian Law and Jurisprudence*, PhD thesis in Private Law, Abou Bekr Belkaid University, Tlemcen, 2016, p. 17.

[3] Mujahideen Khaled, *The Concept of Public Order in Contracts*, PhD thesis, Faculty of Legal, Economic and Social Sciences, Hassan II University, Casablanca, Morocco, 2005, p. 43.

[4] Alyan Bouziane, *The Impact of Public Order on the Exercise of Public Freedoms – A Comparative Study between Islamic Law and Algerian Law*, PhD thesis, Faculty of Political Science and Islamic Civilization, University of Oran, 2007, p. 4.

operates within the framework of this system without being able to transgress it. Although this system shares certain features with other forms of social regulation and human conduct, it has gradually acquired distinct dimensions that have transformed it into a specific intellectual construct, later known as public order.[5]

The rules of public order are those intended to achieve a political, social, or economic interest related to the organization of society [6], which prevails over individual interest. All individuals are therefore required to respect and uphold this interest, and they are not permitted to contravene it through agreements among themselves, even if such agreements serve their personal interests. This is because public interests take precedence over private interests. Consequently, any agreement that departs from this system is deemed null and void.

The concept of public order permeates all aspects of the general theory of law. It occupies a prominent position across the various branches of law, both public and private. In public law, it represents an objective pursued by legislative, administrative, and judicial regulatory authorities, aimed at ensuring public security, safeguarding public health, and maintaining public tranquility. In private law, it consists of a set of legal rules governing the fundamental and essential interests of society, embodied in mandatory and prohibitive rules that individuals may not violate, either immediately or in the future. This is because these rules concern the interests of society more directly than those of individuals, and therefore constitute a fundamental restriction on contractual freedom.

Accordingly, the concept of public order, in this functional sense, cannot be confined to a specific domain. Rather, it is a dynamic and evolving notion that expands or contracts according to what is considered a public interest within a given civilization. It tends to be narrowly defined within socialist or social doctrines that prioritize collective interest above all else, often at the expense of individual interest.

2- Determining the Meaning of Public Order in Algerian Law:

An examination of the evolution of the idea of public order shows that this concept is not relatively recent, but rather has deep historical roots in positive legal systems, particularly since the beginning of the nineteenth century. The development of this concept has gradually contributed to clarifying and shaping its meaning, until it has become a cornerstone of all positive legal systems.

Given that Algerian law is relatively recent compared to other legal systems, particularly Latin systems, it is undeniable that the Algerian legislator drew the concept of public order from these systems, foremost among them French law, especially civil law. Therefore, determining the meaning of public order in Algerian law cannot be achieved without first examining the concept within French legislation.

Although French law has adopted the concept of public order, it has not provided a precise definition of it. This opened the way for French legal doctrine to define and conceptualize public

[5] Imad Tarek El-Bishry, previous reference, p. 51.

[6] Abdel Moneim Farag El-Sadda, *Principles of Law*, Dar Al-Nahda Al-Arabiya, Beirut, 1977, p. 59.

order. Algerian law has followed the same approach and has not departed from this path in determining the concept of public order.

The Second Requirement: The Concept of Public Morals

Anyone seeking to understand the concept of public morals must first grasp its relationship with public order. In order to fully apprehend the idea of public morals, we have deemed it necessary, within this section, to clarify the sources of public morals in accordance with Algerian legislation, beginning with its definition and extending to its sources.

First Branch: Definition of Public Morals

Public morals constitute, in the life of different societies, a fundamental pillar for the stability of individuals within their homelands and places of residence. Public morals refer to those standards of conduct that have become customary among individuals in various societies, encompassing the etiquette governing interactions between people across different situations and times.

Public morals represent a set of essential ethical rules necessary for the proper functioning and preservation of society, safeguarding it from moral disintegration. In other words, they constitute the minimum threshold of principles derived from traditions, religious beliefs, and moral values within a society, the violation of which is regarded as deviance and moral decay condemned by the community. Thus, public morals can be understood as the ethical expression of the concept of public order.

Given this nature, the legal rules associated with public morals cannot be considered merely optional or subject to individual discretion. Rather, their violation leads to the collapse of the moral fabric of society. Accordingly, public morals, in this sense, form an integral part of public order.[7]

Similar to the concept of public order, the notion of public morals is also indeterminate, unclear, and theoretically difficult to define with precision. It is likewise a relative concept that varies from one society to another and even within the same society over time.

Although the rules of public morals are connected to both the rules of public order and moral norms enshrined in legal provisions, they differ from them in scope. Public morals primarily concern principles and foundations related to sexual matters; however, they also extend to other issues such as gambling, betting, and the acquisition of money through dishonest means. Public order, by contrast, is broader in scope, encompassing—alongside public morals—the fundamental political, economic, and social principles upon which society is based.

The Second Section: Public Order and Public Morals in the Digital Environment in Relation to the Electronic Signature

The most significant threat to electronic transactions—particularly within the sphere of electronic commerce—is the compromise of information security and the failure to adequately secure the electronic signature. Such vulnerabilities lead to a threat to public order and public morals by undermining the integrity of information exchange, whether through interference by a third party or any entity other than the contracting parties. Consequently, it became necessary to establish

[7] Imad Tarek El-Bishry, previous reference, p. 50.

mechanisms that ensure the confidentiality and protection of data, so that no one—except the contracting parties or those authorized by law—can access it. [8]

The First Requirement: Protection of Privacy

The disclosure of information or secrets refers to their dissemination, transfer, or exposure to third parties, making them known to a wider audience and removing them from the realm of confidentiality after knowledge of them had been restricted to their holders or to those who had access to them by virtue of their functions, namely electronic certification service providers and their assistants. [9]

The protection of privacy in the context of electronic signatures is linked to an integrated framework that defines the elements and scope of such protection. This framework is embodied in five fundamental principles governing what are referred to as ordinary, acceptable, or fair practices in the field of information privacy or personal data protection, namely: notice (notification), choice, access to data, enforcement, and security. [10]

Notice (Notification): This principle entails the obligation of the service provider or website to inform users if the website or the nature of the service involves the collection of personal data, as well as to specify the extent to which such data are collected and used.

Choice: This principle requires companies that operate websites or provide services to offer users the option regarding the use of their data for purposes other than those for which they were originally collected. [11]

Access to Data: This principle obliges granting users the ability to access their data, verify their accuracy, and update them when necessary. [12]

Security: The content of this principle concerns the obligations imposed on service providers and websites, particularly with regard to security standards, data confidentiality, proper usage integrity, and the prohibition of unauthorized access to such data. It also encompasses mechanisms such as passwords, encryption, and other information security tools.[13]

Enforcement of the Law: This principle relates to the imposition of sanctions on entities that fail to comply with the aforementioned principles. [14]

Within this framework, automated data processing systems—including electronic signatures and electronic certification certificates—have been granted criminal protection by the Algerian legislator as part of safeguarding privacy and the confidentiality of information.

---

[8] Belhassine Hamza, previous reference, p. 75.

[9] Abdel Fattah Al-Bayoumi Hijazi, *Electronic Commerce in the Arab Model Law for Combating Computer and Internet Crimes*, Dar Al-Kutub Al-Qanouniya, Egypt, 2007, pp. 89–90.

[10] Ayman Ramadan Mohamed Ahmed, previous reference, p. 101.

[11] Yasser Mohamed Al-Koumi Mahmoud Abu Hatab, *Criminal Security Protection of the Electronic Signature*, Mansha'at Al-Ma'aref, Alexandria, 2014, p. 102.

[12] Yasser Mohamed Al-Koumi Mahmoud Abu Hatab, previous reference, p. 102.

[13] Law No. 16/01 dated 06 March 2016, Official Gazette No. 14, concerning the amendment of the Constitution.

[14] The electronic document is defined as any independent entity or separable component from an automated data processing system containing recorded data—Ayman Abdallah Fikri, previous reference, p. 382.

Beginning with the Constitution, Article 46, in its fourth paragraph, provides as follows: "The confidentiality of correspondence and private communications in all their forms is guaranteed. The protection of natural persons in the processing of personal data is guaranteed by law, and any violation thereof shall be punishable."

In the Penal Code, pursuant to Article 394 bis and the following provisions, particularly Article 394 bis 2, which concerns the possession, disclosure, or use of such data for any purpose, the law criminalizes acts relating to organized data stored in information banks that contain private and confidential information belonging to individuals. Accessing, revealing, or disseminating such data is considered an offense, as part of the protection of the right to privacy.

In the same context, Articles 61, 68, and 73 of Law No. 15/04 relating to electronic signature and electronic certification, as previously mentioned, criminalize the possession, acquisition, or use of electronic signature creation data that specifically belong to another person. This constitutes a form of protection for confidential privacy and ensures the integrity of the electronic signature. Likewise, Articles 42 and 43 address the obligations imposed on certification service providers.

First Branch: The Overlap Between the Protection Afforded to the Electronic Signature and the Criminal Protection of Secrets

This overlap is reflected in the possibility of distinguishing between offenses affecting the electronic document [15] and the disclosure of secrets. The act of disclosing a secret must be committed by a person entrusted with preserving that secret, unlike offenses affecting the electronic document, which may be committed by any individual. On the one hand, even where the offense does not require disclosure by a person entrusted with the secret, a distinction between the two concepts remains. On the other hand, the notion of "secret" in crimes of disclosure is narrower in scope than the concept of confidentiality of a document. The law protects the secret regardless of the form in which it is preserved. [16]

From the foregoing, it becomes clear that the concept of electronic data is broader in scope than the notion of secrecy, which is primarily linked to the professional or functional duties of those entrusted with it.

Most legislations limit themselves to criminalizing the means by which the right to confidentiality of electronic signature data is violated, leaving the determination of the content of this right to the victim. Meanwhile, comparative jurisprudence and case law tend to establish criteria for defining what constitutes a "secret," the disclosure of which constitutes a breach of the obligation to preserve it.

The legal protection of privacy and confidentiality in the exchange of electronic signature data gives rise to several aspects, including:

[15] Sophie Bardou, *Les traitements de données biométriques en entreprise*, doctoral thesis, University of Montpellier 1, November 2010, p. 111.

[16] Ayman Ramadan Mohamed Ahmed, previous reference, pp. 102–103.

First: Protection of Trust in the Electronic Signature

The principle of the credibility of the electronic signature relates to the extent of its evidentiary value in electronic transactions of various forms, particularly in light of the risks affecting information security and the lack of adequate protection for the electronic signature process. This, in turn, undermines the integrity of the exchange of information necessary for the conclusion of electronic contracts.

This is due to the possibility of breaching computer systems, discovering or decrypting electronic signatures, or seizing and using them without the consent or knowledge of their owners. This situation is further aggravated by the forgery of credit cards and the continuous development of malicious software such as viruses, which may destroy or alter files stored within information systems, thereby disrupting transactions and causing a loss of credibility. [17]

In addition, considerable efforts have been directed toward overcoming the obstacles facing electronic transactions through the adoption of electronic writing, which is fundamentally based on electronic documents, as well as through the recognition of the electronic signature and its equivalence to the handwritten signature.

In this regard, the issuance of the UNCITRAL Model Law on Electronic Commerce, adopted by the United Nations Commission on International Trade Law on December 1, 1966, granted electronic messages and data legal evidentiary value and recognized the electronic signature, equating it with the handwritten signature. [18]

Furthermore, during its thirty-fourth session, the United Nations Commission on International Trade Law developed the UNCITRAL Model Law on Electronic Signatures of 2001. This law provides a regulatory framework for certified electronic signatures, identifies the authority responsible for their validation, sets forth the obligations of the signatory, and regulates electronic signature certification services and electronic certification certificates, including the recognition of foreign electronic signatures and certificates.

The Algerian legislator has also devoted particular attention to the electronic signature and has explicitly recognized its evidentiary equivalence to the traditional handwritten signature through the issuance of the aforementioned Law No. 15/04 relating to electronic signature and electronic certification. Within this framework, numerous safeguards have been established to ensure the necessary level of trust for all participants in electronic transactions, while preventing the imitation, forgery, or manipulation of electronic signatures.

Second: Legitimacy of the Circulation of Electronic Signature Data

One requirement for the lawful circulation of data in the field of electronic signature and electronic certification is that such circulation must take place through an authorized electronic service provider. This principle is expressly established by the Algerian legislator in Law No. 15/04 relating to electronic signature and electronic certification, particularly in Article 33 and the following provisions, where such activities are subject to a licensing regime. Article 33 provides that: “The

[17] Yasser Mohamed Al-Koumi Mahmoud Abu Hatab, previous reference, p. 105.
[18] Yasser Mohamed Al-Koumi Abu Hatab, previous reference, p. 101.

activity of providing electronic certification services shall be subject to authorization granted by the economic authority for electronic certification."

In this regard, the Algerian legislator has imposed an obligation on electronic certification service providers to inform the economic authority for electronic certification, within the time limits specified in the certification policy, of their intention to cease activities relating to the provision of electronic certification services, or of any act that may lead to such cessation. This is in accordance with Articles 58 and 59 of the aforementioned Law No. 15/04. The service provider is also required to ensure service continuity. The cessation of its activities results in the withdrawal of the license granted to it, as stipulated in Articles 67, 71, 72, and 74 of the same law. Any breach of these procedures gives rise to criminal liability.

The protection granted to electronic signature and electronic certification may, in certain respects, resemble the protection afforded to computer operating systems. The similarity lies in the fact that, in both cases, the object of infringement concerns the data contained in the signature, the electronic certification certificate, or the operating program. This resemblance has led some scholars to argue that electronically processed data cannot be separated from the programs that regulate them, and that both therefore share the same nature as a single intangible entity. Consequently, the protection of such programs also constitutes protection for electronically processed data. [19]

First Branch: Fields of Criminal Protection of the Electronic Signature

The concept of electronic signature and electronic certification is closely connected to numerous vital domains within state institutions, as well as to various civil and commercial transactions. These areas necessarily require deterrent legal protection that intersects with the protection granted to electronic signatures and certifications. This will be examined through the criminal protection afforded to e-government, electronic commerce, and other related civil transactions.

The Second Requirement: The Intervention of Law No. 15-04 Relating to Electronic Signature and Electronic Certification in the Protection of Public Order and Public Morals

In traditional legal frameworks, the primary function of a signature is to identify the signatory and express their will. Over time, the signature has taken various forms, culminating in the electronic signature, which is now embedded in different forms of contractual relations conducted via the Internet. It therefore became necessary to regulate it, define its forms, establish its conditions and requirements, and ensure its legal recognition in order to guarantee its evidentiary value. Without such recognition, the electronic signature cannot benefit from any form of legal protection.

First Branch: Definition of Electronic Signature and Electronic Certification

The electronic signature is among the applications that have emerged and expanded in use as a result of the growing reliance on computer technologies. [20]Given that electronic documents, including contracts, are concluded remotely between parties who may not know one another, it has

[19] Abdel Fattah Al-Bayoumi Hijazi, *Electronic Signature in Comparative Legal Systems*, Dar Al-Fikr Al-Jami'i, Egypt, 2005, p. 11.

[20] Belhassine Hamza, *Legal and Technical Protection of the Electronic Signature*, Journal of Legal and Administrative Sciences, Issue 11, p. 83.

become essential to provide guarantees and mechanisms that ensure the identification of the contracting parties and reliably confirm their identity, thereby enabling legal acts to be attributed to their rightful authors. [21]

There also arose a need for the involvement of a trusted and neutral third party capable of verifying, through specific procedures, the authenticity of electronic signatures. This entity is referred to as the certification authority or the electronic certification service provider. [22]

First: Definition of the Electronic Signature

A signature, in general, is a written mark that allows its holder to be identified, distinguishes them from others, and expresses their intention to approve the content of a legal act.

The electronic signature, as a relatively recent linguistic and legal term, refers to a process carried out through electronic means for the purpose of authentication and identity verification, while also expressing the will of the signatory. [23]

- **Doctrinal Definition**

Legal scholars have provided multiple and varied definitions of the electronic signature. Some have approached it from a technical perspective, focusing on the manner in which it is created and defining it accordingly, while others have adopted a functional perspective, focusing on its purpose and defining it on that basis. [24]

Among these definitions is the following: "Any signs, symbols, or characters authorized by the competent authority for signature accreditation, which are closely linked to a legal act, enabling the identification of their holder and the determination of their identity, and expressing, without ambiguity, their consent to that legal act." [25]

Others consider the electronic signature to be "a specific procedure carried out by the person intending to sign a document, whether this procedure takes the form of a number, a particular electronic signal, or a special code, such that the number or code is used in a secure and confidential environment preventing its use by others, thereby providing assurance that it originates from its holder, namely the person possessing the number or code." [26]

Some scholars also distinguish between the electronic signature and the digital signature. They argue that the electronic signature consists of a sequence of numerical values, zeros and ones, whose combination forms the digital electronic signature.

As for the digital signature, it consists of printed numerical values referred to as (HASH), representing the content of the transaction being signed. [27]

---

[21] Belhassine Hamza, previous reference, p. 83.

[22] Ibrahim Ibn Satam Bin Khalaf Al-Anzi, *Electronic Signature: Its Forms and Applications*, PhD thesis, Riyadh, 2009, p. 37.

[23] Ibrahim Ibn Satam Bin Khalaf Al-Anzi, previous reference, p. 38.

[24] Tharwat Abdel Hamid, *Electronic Signature: Its Nature and Risks*, Dar Al-Jami'a Al-Jadida, 2007, p. 50.

[25] Najwa Abu Haiba, *Electronic Signature: Definition and Evidentiary Value*, Cairo, 2004, p. 41.

[26] Mohamed Amin Al-Roumi, previous reference, p. 15.

[27] Ayman Ramadan Mohamed Ahmed, *Criminal Protection of Electronic Signature*, p. 30.

In light of this, French legal doctrine and jurisprudence have established that the electronic signature performs two essential functions: first, it identifies the signatory; and second, it expresses the signatory's intention through approval of the content of the legal act. [28]

• Legal Definition:

The Algerian legislator defined the electronic signature in Article 02, paragraph (01), of Law No. 15/04 issued in 2015 concerning electronic signature and electronic certification as "data in electronic form, attached to or logically associated with other electronic data, used as a means of authentication." [29]

It had previously been recognized under Article 327/2 of Law No. 05/10 dated 20 June 2005[30], which provides that the electronic signature shall be deemed valid under the conditions set out in Article 323/1, namely the possibility of verifying the identity of the person who issued it, and that it is created and preserved under conditions ensuring its integrity. [31]

The definition adopted by the Algerian legislator is, to a considerable extent, consistent with the definition provided by the UNCITRAL Model Law of 2001, which defines it as: "data in electronic form contained in, or attached 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." [32]

Similarly, Article 1416/4 of the amended French Civil Code, introduced by French Electronic Signature Law No. 24/2000 issued on 14 April 2000, defines the signature in general as: "the signature necessary for the completion of a legal act, which identifies the person who affixed it and expresses their consent to the obligations arising from such act. When it is electronic, it must be created using a reliable means that ensures the identification of the signatory and guarantees its link to the act to which it is affixed." [33]

United States federal law defines the electronic signature as: "an electronic sound, symbol, or process attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record." [3435]

Furthermore, the legislator in the State of New York introduced an amendment to the Electronic Signatures and Records Act issued on 6 August 2002, providing a definition of the electronic signature as "an electronic sound, symbol, or process attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign such record." [36]This definition closely aligns with that provided by the German legislator in Article 2 of the Electronic

---

[28] Law No. 15/04 dated 01 February 2015, Official Gazette No. 06.
[29] Law No. 05/10 dated 20 June 2005, Official Gazette No. 44.
[30] Saleh Shanin, *Criminal Protection of Electronic Commerce*, PhD thesis, Tlemcen, 2013, p. 52.
[31] UNCITRAL Model Law on Electronic Signatures 2001, Article 2/BF.
[32] French Law No. 2000-230 of 13 March 2000.
[33] U.S. E-Sign Law 106(5), report p. 11.
[34] Kansas electronic signature definition.
[35] ESRA 102(3), report p. 7 note 3.
[36] Draft framework law, 2(2), p. 4.

Signature Act[37], which distinguishes between the ordinary electronic signature and the advanced electronic signature. Both share the characteristic of being electronic data attached to or logically associated with other data and used to authenticate their attribution to a specific person. [38]

However, the advanced electronic signature, according to the German legislator, is subject to more stringent requirements than the ordinary one. It involves a code exclusively assigned to a specific individual, not shared with others, and is capable of identifying its user. It must also ensure that the signatory retains exclusive control over the signature creation data, and that any subsequent alteration of the signature data can be detected. [39]

In the same context, the Egyptian legislator, in Law No. 15/2004 on electronic signature issued on 22 April 2004, defined the electronic signature as: "that which is affixed to an electronic document and takes the form of letters, numbers, symbols, signs, or otherwise, possessing a unique character that allows the identification of the signatory and distinguishes them from others." [40]

Second: Definition of Electronic Certification

Transactions conducted over the Internet take place within an open network that lacks any physical presence, which makes the process of identifying the individuals involved in communication within this virtual environment particularly difficult. At the same time, it facilitates acts such as identity theft, interception of others' communications, and the repudiation of transactions such as sales, payments, or exchanges. Consequently, the establishment of security mechanisms such as electronic certification has become a necessity. [41]

The Algerian Regulatory Authority for Post and Electronic Communications has defined electronic certification as: "a process that ensures four security aspects of information exchange over the Internet, namely confidentiality, authentication, integrity, and non-repudiation, as these aspects contribute to establishing a climate of trust through the implementation of a public key infrastructure (PKI)." [42]

- **Electronic Certification in Law:**

The Algerian legislator, in Article 2, paragraph 15 of Law No. 15/04, defined the electronic certification policy as: "the set of rules and organizational and technical procedures relating to electronic signature and electronic certification." [43]

Electronic certification is also defined as a secure means for verifying the validity of a signature or document, whereby it is attributed to a specific person or entity. [44]

Electronic certification may further be understood as a set of technical processes and mechanisms, consisting of tools and automated means used to verify the authenticity and identity of the parties

---

[37] Hussein Ben Said Al-Ghafri, *Crimes Affecting Electronic Commerce*.
[38] Draft framework law, 2(2), p. 4.
[39] Egyptian Electronic Signature Law No. 15 of 2004.
[40] ARPT website: www.arpt.dz/ar/gd/ce
[41] Previous reference: www.arpt.dz
[42] Law No. 15/04 dated 10 February 2015.
[43] Ahmed Hussein Mansour, *Electronic Evidence*, p. 209.
[44] Yamina Houhou, *Electronic Sale Contract in Algerian Law*, p. 189.

involved in a transaction. It encompasses various instruments through which the electronic signature is created, as well as those that ensure its integrity and security. [45]

From these definitions, it becomes evident that electronic certification constitutes an integrated process involving multiple mechanisms, commonly referred to as certification or authentication authorities, as well as electronic certification certificates.

Second Branch: The Concept of Electronic Certification Authorities

A certification service provider is defined as: "an entity, whether a public organization or a private independent body, that acts as an intermediary between parties in order to authenticate their electronic transactions through the issuance of electronic certificates." [46]

The third party responsible for carrying out the certification process is referred to as the "certification service provider," commonly abbreviated as (PSC).

The Algerian legislator defined this entity in Law No. 15/04 dated 10 February 2015 [47], specifically in Article 2, paragraphs 11 and 12, where the term "trusted third party" was introduced to indicate that the provision of electronic certification services is limited to legal persons. The legislator also explicitly defined the "electronic certification service provider" in the subsequent paragraph, as follows:

- **Trusted Third Party:** a legal person that issues qualified certification certificates and may provide other services related to electronic certification for the benefit of stakeholders within the governmental sector.
- **Electronic Certification Service Provider:** a natural or legal person that issues qualified electronic certification certificates and may provide other services in the field of electronic certification.

The UNCITRAL Model Law on Electronic Signatures defines the certification service provider in Article (E/2) as: "a person that issues certificates and may provide other services related to electronic signatures." [48]

Similarly, the UAE law defines this entity as: "any person or accredited or recognized entity that issues electronic certification certificates, or performs any services or functions related thereto or to electronic signatures." [49]

Accordingly, the role of certification or authentication authorities consists in verifying the validity and integrity of the electronic signature. It also involves establishing the electronic identity of the contracting parties, as well as their legal capacity to engage in transactions and conclude contracts. Furthermore, these authorities ensure the verification of the content of such transactions in terms of their validity and seriousness, and they are also responsible for issuing electronic keys, whether private or public. [50]

---

[45] Said Al-Sayed Qandil, *Electronic Signature*, p. 75.
[46] Law No. 15/04 dated 10 February 2015.
[47] Article E/2 of UNCITRAL Model Law.
[48] European Official Journal, January 2000.
[49] UAE Electronic Transactions Law No. 12 of 2002, Article 2/20.
[50] Belhassine Hamza, previous reference, p. 84.

Third Branch: The Concept of Electronic Certification Certificates

Electronic certification certificates play an effective role in electronic transactions. They serve to verify the sender's identity, ensure the integrity and accuracy of the data recorded in the document, and guarantee that such data have not been altered. This, in turn, strengthens trust and security among parties conducting transactions via the Internet. [51]

The Algerian legislator defined them in Law No. 15/04 of 2015, paragraph seven, as a document in electronic form that establishes the link between electronic signature verification data and the signatory. [52]

Article 2 of the UNCITRAL Model Law issued by the United Nations defines them as "a data message or other record that confirms the relationship between the signatory and the signature creation data." [53]

Similarly, Article 3 of the European Directive defines the electronic certification certificate as "that which links a signature to a specific person and confirms the identity of the signatory."[54]

From a technical perspective, some scholars define it as an electronic process that associates a specific person (whether a natural or legal person) with particular attributes that distinguish them from others. [55]

It may thus be considered as an electronic identity card issued during the process of creating the electronic signature. [56]

In most legislations, a designated authority is entrusted with issuing such certificates and authenticating the electronic signature simultaneously. By virtue of this certificate, the competent authority can attest to the validity of the signature and thereby determine the identity of the signatory.

The purpose of the electronic certification certificate is to confirm the existence of a link between the signatory and the signature creation data. It also certifies that the electronic writing (or what is referred to in some Arab legislations as a data message) is valid and has not been tampered with [57], thereby ensuring the validity of the electronic signature and its attribution to its issuer, provided that it satisfies the legal, technical, and procedural requirements prescribed by law. Ultimately, it acquires evidentiary value equivalent to that of a handwritten or traditional signature.

Fourth Branch: Electronic Certification Authorities

The Algerian legislator, through Law No. 15/04 mentioned above, established three authorities for electronic certification. Their provisions were regulated in Chapter Three of this law under the title of electronic certification authorities. These authorities are: the National Authority for Electronic

---

[51] Lazhar Ben Said, *Electronic Commerce Contracts*, p. 182.
[52] Law No. 15/04, previous reference.
[53] Abdel Fattah Hijazi, previous reference, p. 261.
[54] Lazhar Ben Said, previous reference, p. 183.
[55] Tulie Nesnault, *La signature électronique*, 2003, p. 11.
[56] Ayman Saad, *Electronic Signature*, p. 93.
[57] Mohamed Amin Al-Roumi, *Legal System of Electronic Signature*, p. 57.

Certification, the Governmental Authority for Electronic Certification, and the Economic Authority for Electronic Certification.

The legislator defined the functions of each authority in a manner that ensures the promotion and development of the use of electronic signature and electronic certification, while also guaranteeing the reliability of their application. [58]

The National Authority for Electronic Certification:

This is an administrative authority established under the Prime Minister, enjoying independence, legal personality, and financial autonomy, in accordance with Article 16 of Law No. 15/04 mentioned above. Its primary mission consists in developing an electronic certification policy and ensuring its implementation, as well as preparing and proposing draft legislative and regulatory texts related to electronic signature and electronic certification. [59]

The Governmental Authority for Electronic Certification:

This authority is established under the minister responsible for postal services and information and communication technologies. It enjoys legal personality and financial independence pursuant to Article 26 of Law No. 15/04. Its responsibilities include monitoring and supervising electronic certification and ensuring the provision of such services for stakeholders within the governmental sector. It is also tasked with preparing the regulatory and technical rules and procedures related to electronic signatures and ensuring their implementation, subject to the approval of the National Authority. [60]

The Economic Authority for Electronic Certification:

This authority is considered the most significant among the electronic certification authorities, as it functions as a regulatory body under the Authority for Regulation of Post and Electronic Communications. The Algerian legislator expanded its powers under Law No. 15/04 by granting it the authority to issue licenses to electronic certification service providers, to take all necessary measures to ensure service continuity in the event of a provider's inability to deliver its services, and to exercise arbitration powers in disputes arising between certification service providers themselves or between providers and users. It is also empowered to notify the public prosecution of any criminal acts discovered in the course of performing its duties.

Conclusion:

Algeria faces significant challenges in the field of digital transformation, including the implementation of e-government requirements, the establishment of a digital economy based on electronic commerce, and the protection of the digital consumer. These objectives can only be achieved through the provision of an adequate legal framework and the continuous integration of advanced technological tools, foremost among them the mechanisms of electronic signature and electronic certification.

---

[58] Belhassine Hamza, previous reference, p. 86.
[59] See Article 188 of Law No. 15/04.
[60] See Article 28 of Law No. 15/04.

At the same time, the improper use of electronic signature and electronic certification highlights the close connection between this legal framework and the necessity of preserving public order and public morals within the digital environment, in order to prevent any manipulation of electronic signature data and various certification services. Such risks may have adverse effects on the national economy, as well as on individuals and society as a whole, and may negatively impact the growing trust of the digital consumer in electronic signature services.

List of References:

In Arabic:

- **Constitutions**
- Presidential Decree No. 20/442 dated 30 December 2020, Official Gazette (J.O.) No. (82) dated 30 December 2020, concerning the amendment of the Constitution.
- **Laws:**
- Law No. 05/10 dated 20/06/2005 amending and supplementing Ordinance No. 75/58 dated 26/09/1975, concerning the Civil Code as amended and supplemented, Official Gazette No. 44 dated 26/06/2005.
- Law No. 15/04 dated 01 February 2015 defining the general rules relating to electronic signature and electronic certification, Official Gazette No. 06 dated 10/02/2015.
- **Foreign Legal Texts:**
- Egyptian Electronic Signature Law No. 15 of 2004, Official Gazette No. 17 (Supplement 3), issued on 22/04/2004.

Books:

- Ahmed Hussein Mansour, *Electronic Evidence*, Dar Al-Fikr Al-Jami'i, Alexandria, 2006.
- Ayman Saad, *Electronic Signature*, Dar Al-Nahda Al-Arabiya, Cairo, 2013.
- Ayman Abdallah Fikri, *Cybercrime: A Comparative Study in Arab and Foreign Legislations*, Law and Economics Library, Riyadh, 2015.
- Said Al-Sayed Qandil, *Electronic Signature*, Dar Al-Jami'a Al-Jadida, Egypt, 20060.
- Abdel Fattah Al-Bayoumi Hijazi, *Electronic Commerce in the Arab Model Law for Combating Computer and Internet Crimes*, Dar Al-Kutub Al-Qanouniya, Egypt, 2007.
- Abdel Fattah Al-Bayoumi Hijazi, *The Legal System for the Protection of Electronic Commerce*, Book One: The Electronic Commerce System and Its Civil Protection, Egypt, 2005.
- Abdel Fattah Al-Bayoumi Hijazi, *Electronic Commerce and Its Legal Protection*, Book One, Dar Al-Kutub Al-Qanouniya, Egypt, 2007.
- Abdel Fattah Al-Bayoumi Hijazi, *Electronic Signature in Comparative Legal Systems*, Dar Al-Fikr Al-Jami'i, Egypt, 2005.
- Abdel Fattah Al-Bayoumi Hijazi, *Procedural Aspects of Preliminary Investigation in Cybercrime: A Comparative Study in Light of General Rules of Criminal Procedure*, Dar Al-Nahda Al-Arabiya, Egypt, 1st ed., 2009.

- Abdel Fattah Al-Bayoumi Hijazi, *Procedural Aspects of Preliminary Investigation in Cybercrime: A Comparative Study in Light of General Rules of Criminal Procedure*, 1st ed., Dar Al-Nahda Al-Arabiya, Cairo, Egypt, 2003.
- Abdel Fattah Al-Bayoumi Hijazi, *Principles of Criminal Procedure in Computer and Internet Crimes*, 1st ed., Dar Al-Fikr Al-Jami'i, Alexandria, 2006.
- Abdel Fattah Al-Bayoumi, *Electronic Commerce and Its Legal Protection*, Book Two: Criminal Protection of the Electronic Commerce System, Dar Al-Kutub Al-Qanouniya, Egypt, 2007.
- Abdel Fattah Hijazi, *Criminal Evidence and Forgery in Computer and Internet Crimes*, Dar Al-Kutub Al-Qanouniya, Cairo, 2002.
- Abdel Fattah Al-Bayoumi Hijazi, *E-Government*, Book Two, Dar Al-Kutub Al-Qanouniya, Egypt, 2007.
- Lazhar Ben Said, *The Legal System of Electronic Commerce Contracts*, Dar Houma, Algeria, 2012.
- Mohamed Amin Al-Roumi, *The Legal System of Electronic Signature*, Dar Al-Kutub Al-Qanouniya, Egypt, 2007.
- Najwa Abu Haiba, *Electronic Signature: Its Definition and Its Evidentiary Value*, Dar Al-Nahda Al-Arabiya, Cairo, 2004.
- Yasser Mohamed Al-Koumi Mahmoud Abu Hatab, *Criminal Security Protection of the Electronic Signature*, Mansha'at Al-Ma'aref, Alexandria, 2014.
- Yamina Houhou, *Electronic Sale Contract in Algerian Law*, Dar Belqis, Algeria, 2016.
- Lazhar Ben Said, *The Legal System of Electronic Commerce Contracts*, Dar Houma, Algeria, 2012.

Articles:

- Hussein Ben Said Ben Youssef Al-Ghafri, *Crimes Affecting Electronic Commerce*, published on the Al-Minshawi website for studies and research.

Theses and Dissertations:

Doctoral Theses:

- Ibrahim Ibn Satam Bin Khalaf Al-Anzi, *Electronic Signature: Its Forms and Applications*, PhD thesis, Naif Arab University for Security Sciences, College of Graduate Studies, Department of Criminal Justice, Riyadh, 2009.
- Alyan Ouda, *The Concept of Public Order and Freedom of Contract in Light of Algerian Law and Jurisprudence*, PhD thesis in Private Law, Abou Bekr Belkaid University, Tlemcen, 2016.
- Mujahideen Khaled, *The Concept of Public Order in Contracts*, PhD thesis, Faculty of Legal, Economic, and Social Sciences, Hassan II University, Casablanca, Morocco, 2005.

- Alyan Bouziane, *The Impact of Public Order on the Exercise of Public Freedoms: A Comparative Study between Islamic Law and Algerian Law*, PhD thesis, Faculty of Political Science and Islamic Civilization, University of Oran, 2007.

Websites:

- Website of the Regulatory Authority for Post and Electronic Communications: WWW.ARPT.DZ
- http://www.signelec.com-le
- minchaoui.com

In Foreign Languages:

- **Foreign Legal Texts:**
- Egyptian Electronic Signature Law No. 15 of 2004, Official Gazette No. 17 (Supplement 3), issued on 22/04/2004.