International Journal of Law and Jurisprudence
Volume 15 · Issue 2 · 2026 · Pages 1950–1959
e-ISSN 2255-1824 (Online) · revistaidj.com/IJLJ

The Impact of Digitisation on Proving Civil Transactions Under Algerian Law No. 26-02

Aroura Fatiha

Lecturer Class A, Faculty of Law, University of Algiers 1, Laboratory of Digital Economy, Green Economy and Business Law, Algeria, Email: f.aroura@univ-alger.dz

Received: 21 March 2026 | **Accepted:** 19 August 2026 | **Published:** 25 October 2026

Abstract

The tremendous development witnessed in the Information and Communication Technology sectors, along with their remarkable integration, has clearly had a positive impact on the widespread adoption of digitisation and the establishment of electronic commerce features. This has represented a civilisational and qualitative leap across all sectors in various countries.

Currently, various sectors primarily rely on information systems and digitisation to carry out their work due to the speed and accuracy with which information can be collected. This reliance is based on electronic means and techniques. This article attempts to address the most significant issue encountered in electronic civil transactions: proof. This is achieved by examining a new type of signature: the electronic signature. The article considers the evidentiary value of electronic signatures in proving civil transactions in light of the new legal provisions introduced by Law No. 26-02. This law sets out the rules relating to trust services for electronic transactions and introduces a new electronic framework in Algeria.

Keywords: information revolution, electronic commerce, information systems, electronic signature, proof of civil transactions.

Introduction

Electronic civil transactions are based on the use of electronic means, including the exchange of information and negotiations, as well as the conclusion of electronic contracts. All of these transactions take place via electronic technologies over the internet and other channels[1]. However, these transactions face the same set of problems as electronic commerce in general, particularly the question of how to prove transactions and acts carried out through modern means of communication. The absence of standards and legal regulations that clarify the legal nature of data and allow it to be accepted as evidence has raised numerous legal questions.

Furthermore, the technical and technological development of modern communication methods has led to a new type of writing and signature characterised by an electronic nature. Furthermore, the use of modern technologies to conclude contracts, especially online, has created a real problem that has made it necessary to reconsider traditional principles of evidence[2]. This is particularly significant given the shift from paper to electronic media. For electronic proof to be effective, the state must recognise the probative value of electronic writing and signatures in proving electronic civil transactions, something the Algerian legislator initially achieved by issuing a special law on electronic signatures and certification[3]. This law was later repealed and replaced by Law No. 26-02, which sets out general rules relating to trust services for electronic transactions and electronic identification[4].

Writing is not considered complete evidence unless it is signed, which is the second element of documentary evidence originally prepared for proof. In this context, signatures have come to occupy a broad field across various branches of public and private law, thanks to their ability to identify the signatory and express their intent.

Initially, signatures were made using stamps. They later evolved into handwritten signatures before expanding to include fingerprint imprints, which are highly effective in identifying the signatory. However, as communication and technology developed, and electronic commerce emerged alongside the major progress it brought to all fields, particularly civil transactions, it became necessary to create signatures consistent with this new reality. This is how the electronic signature appeared. Rather than taking a single form, it adopted several, starting with signatures via secret codes and progressing to digital signatures, which have gained wide recognition in the field of electronic transactions[5].

Accordingly, this study focuses on the most important issues related to electronic proof, particularly the electronic signature, given its significance in civil transactions. The study also aims to highlight the new legal provisions introduced by the Algerian legislator in Law No. 04-15, which sets out the general rules relating to electronic signatures and certification. The study attempts to answer a central question: What is an electronic signature and what evidentiary value does it have in proving

electronic civil transactions according to the provisions of Law No. 15-04?

To answer this question, it is necessary to consider a number of elements, including what is meant by an electronic signature and the forms it can take. What conditions must be met for it to be valid and legally recognised? Finally, what is the extent of its legal evidentiary authority? The answers to these questions will be provided in the following sections.

Chapter One: The Concept of the Electronic Signature

The emergence of the electronic signature as a new term necessitates clarifying what this concept means by examining the 2001 Model Law on Electronic Signatures and certain related legislation. First, this analysis will focus on Algerian legislation, and then, in a second stage, it will identify the types or forms of this signature. Finally, the third stage will explain the legal conditions that must be met to give it legal recognition, in light of Law No. 15-04.

First requirement: Definition of the electronic signature

In light of the significant technological development and the widespread use of electronic processing systems, the traditional forms of signature no longer have a place. This has led to electronic signatures becoming an alternative to traditional signatures: they perform the same functions and adapt to modern administrative means.

Several definitions of electronic signatures have been proposed at various levels, including international organisations, legal legislation and scholarly (jurisprudential) definitions.

Several international organisations have addressed the definition of electronic signatures through electronic commerce laws or laws created specifically for electronic signatures. The most important of these are:

- the United Nations Commission on International Trade Law (UNCITRAL)[6].

- the European Union as a regional organisation[7].

Article 2(a) of the 2001 UNCITRAL Model Law on Electronic Signatures defines the electronic signature as follows:

‘Electronic data in the form of information incorporated into a data message or logically associated with it, which can be used to identify the signatory and indicate their approval of the information contained in the data message[8].’

The following can be observed from this definition:

Firstly, it did not specify the method used to create the signature, which is a positive approach aimed at allowing room for any suitable method[9].

Second, this definition focused on the requirement for an electronic signature to perform the functions of a signature, namely identifying the signatory and expressing their approval of the information contained in the data message. In any case, every signature, regardless of the method used to create it, must fulfil these functions.

The European Union directives addressed two types of electronic signature, providing a specific definition for each:[10]

1) Simple/ordinary electronic signature: information in electronic form that is closely associated with other electronic information and uses a documentation (authentication) tool.

2) Advanced electronic signature: this is an electronic signature that must satisfy precisely defined requirements.

In terms of legal legislation, there are several definitions of electronic signatures. One of the most important is French legislation, which adopted a functional definition of signature in general. This is set out in Article 1316, paragraph 4, of the French Civil Code, as amended by Law No. 230-2000[11], which states the following:

‘A signature identifies the person to whom it is attributed, indicating their acceptance of the content of the document to which it is attached and the obligations contained therein[12].’

French law further defines the electronic signature in the second paragraph of the amendment as follows:

‘a signature resulting from the use of any reliable and acceptable means for identifying the signatory, and which ensures the link between the signature and the document or work to which it is attached.’

Similar to the Egyptian legislator, the Algerian legislator also addressed the electronic signature and devoted specific legislation to it through Law No. 04-15 relating to electronic signatures and certification[13]. Article 2 (second paragraph) defines it as follows:

‘Data in electronic form, attached to or logically associated with other electronic data, and used as a means of authentication (proof of authenticity)’.

Paragraph three of the same article further adds that:

‘Signature creation data for an electronic signature are unique data, such as symbols or private encryption keys, which the signatory uses to create the electronic signature.’

This definition is essentially the same as that contained in Article 2 of Law No. 26-02, which defines an electronic signature as:

‘Data in electronic form that is attached to, or logically associated with, other data in electronic form that the signer uses to sign, and which is used as an authentication method.’

From this definition, it can be observed that:

First, it indicates that the electronic signature takes the form of data with no specific fixed form, as it states that it may be 'unique data such as symbols or private encryption keys'.

Secondly, the definition requires that the data be included in electronic form or logically linked to other electronic data because this is an electronic signature.

Thirdly, the Algerian legislator required that this data be used for authentication purposes. This means it must enable the identification of the signatory and provide proof of their acceptance of the content of the writing. This is confirmed by Article 6 of this law, which states that:

'The electronic signature is used to authenticate the identity of the signatory and to prove their acceptance of the content of the writing in electronic form.'

From a doctrinal perspective, legal scholarship has provided many definitions of the electronic signature. Some define it as:

'a specific procedure carried out by the person intending to sign the document, whether this procedure takes the form of a number, a particular electronic sign or a special code[14]'. The important point is that the number or code is securely and confidentially stored in a way that prevents its use by others and provides assurance that this signature indeed originates from its holder, i.e. the person who possesses the number or code. Accordingly, the electronic signature may be referred to as a procedural signature[15].'

Others define it as:

'The signature resulting from following specific procedures that ultimately lead to a known result in advance; the set of these procedures constitutes the modern alternative to the traditional concept of a signature[16].'

Thus, an electronic signature consists of encrypted data segments relating to the message, which are sent alongside the message. Verification involves decrypting the signature and comparing its contents with those of the message[17].

According to various definitions, the electronic signature performs the same functions as the traditional handwritten signature. However, some argue that electronic signatures provide greater security than traditional signatures because they rely heavily on encryption technology, meaning that electronic signatures are known only to their owners[18]. Additionally, traditional signatures are easier to forge than electronic signatures. Furthermore, a traditional signature can be detached from the document containing it; this is not possible with an electronic signature, as it forms part of the encrypted document. Furthermore, in order to decrypt it, the signature must correspond to the document.

The primary reason for recognising and adopting electronic signatures is that electronic commerce in general and electronic civil transactions in particular, carried out via the internet and modern means of communication, require security and privacy on the network, as well as the preservation of information and data relating to customers — especially when they use various electronic payment methods. For instance, electronic money transfers are conducted using keys attached to messages alongside electronic signatures[19].

The second requirement: Images of electronic signatures

When we talk about electronic signatures, we are not referring to a signature that appears in a single form. Just as the traditional signature can take several forms, the electronic signature can also take multiple forms, or 'images', which are unified by their use of electronic media and modern technologies capable of converting distinctive personal characteristics, such as numbers and letters, into unique data for signing electronic documents and contracts.

Modern technologies have produced various types of electronic signature. The most important of these are as follows:

A. Signature based on personal (biometric) characteristics: *Signature biométrique*

Biometric signatures are created using one of each person's distinctive characteristics — by relying on their behavioural or physical traits — in order to distinguish and identify them. Therefore, it is referred to as a signature based on personal characteristics.

This form of electronic signature is based on the scientific fact that each person has unique inherent traits that differ from person to person and are characterised by a relatively stable nature. This lends credibility to the notion that a signature employing one of these characteristics has been produced by the signatory themselves, thereby confirming their identity and bestowing legal authority upon the signature in matters of evidence.

The most important physical traits on which biometric signatures rely are the fingerprint, iris scanning, facial recognition, hand characteristics and voice tone[20].

In this system, the identity of the contracting party is verified by entering information into a computer or other modern device, such as capturing an accurate image of the user's eye, voice or hand. This information is then stored encrypted in the computer's memory so it can be compared and matched[21].

However, this system has several drawbacks. For example, the signature image is stored on the computer's hard drive, which may be vulnerable to hacking. Additionally, this technology cannot be used with all computer devices. Furthermore, substantial investment is required to enable users of electronic networks to employ the signatory's personal characteristics in the electronic signature[22].

Digital (code) signature:

This type of signature uses a secret number known only to the signatory. It is used in both civil and non-civil dealings and in electronic correspondence exchanged between traders or companies. In electronic contracts, it consists of a set of numbers or letters chosen by the signatory and arranged and combined in a specific coded form that determines the identity of the holder. This secret code is known only to the holder[23].

In this sense, a digital electronic signature has several advantages, including:[24]

- It is more reliable than a traditional signature because the digital signature identifies the document being signed in such a way that any alteration is highly improbable.

It allows contracting to take place remotely, without the physical presence of the contracting parties, thereby contributing to the growth of e-commerce and the expansion of electronic civil transactions.

- It is a legal means of identifying the signatory.

This signature emerged as a result of significant developments in encryption science. Accordingly, electronic signatures are based on encryption[25], which can be divided into two types:

Symmetric encryption: this is based on a shared secret number between the two parties. It operates in an isolated environment, such as with banking cards, where the secret number is known only to the cardholder and the card reader[26].

- Asymmetric encryption: It relies on a pair of asymmetric keys: a public key and a private key. The first is known to everyone, whereas the second belongs exclusively to its owner, who keeps it secret and uses it to encrypt their message in such a way that they cannot deny what has been stated therein.

It is worth noting that digital signature codes are generated through mathematical algorithms that transform the written signature into a mathematical equation. This equation can only be reverted to its original form by the person who possesses the corresponding private key/equation[27].

Signing with an electronic pen (pen-op)

This method uses a sensitive electronic pen that can write on a computer screen via a specific programme[28]. The pen captures the signature and verifies its accuracy.

The process works as follows:[29]

First, the programme captures the signature written by the user on a digital tablet using a digital pen, and stores the related data.

Second, The program stores the digital signature and related data using an encryption algorithm.

Thirdly, the stored signature can be used by the user whenever required by integrating the programme's representation of the digital signature into the document or file using a mixing/embedding technique. This technique involves generating a unique sequence of symbols for each digital file. Therefore, any attempt to alter, falsify or tamper with the file's contents will be revealed because the resulting sequence of embedded symbols will change as soon as any symbol within the file changes.

Fourth, The accuracy and validity of the signature are recognised through a programmed system that compares the found signature with the stored one. This comparison is based on a set of biometric characteristics of the signature, including directional rays, pen position data on the tablet, acceleration phases during the signing process, total writing speed, pressure applied to the tablet, time differences, writing directions using negative and positive coordinates, and many other time- and acceleration-related coordinates. The required level of accuracy for the signature can be set between 0% and 100%, depending on the importance of the transaction and document.

Fifth, The digitally signed document is opened using the electronic pen and the program checks the integrity of the signature and the document. If any alterations have been made, a warning message is displayed.

Accordingly, this type of signature serves two purposes:

- Capturing the signature by signing with the electronic pen.
- Verifying the signature's validity by comparing the stored signature with the signature produced using specific biological characteristics[30].

However, it is worth noting that, in the context of e-commerce and electronic civil transactions, more emphasis is placed on digital signatures, i.e. those obtained using a secret code (password).

Nevertheless, Article 3 of the 2001 UNCITRAL Model Law on Electronic Signatures established the principle of equivalent treatment of signature technologies. This means that all technologies should have the same opportunity to meet legal requirements. Therefore, no preference should be given to one signature method over another, nor should different types of messages or electronically signed instruments be treated differently, provided the legal requirements are met. Nevertheless, this does not affect individuals' freedom, since they remain entitled to agree among themselves to exclude certain electronic signatures.

The third requirement: Conditions for the Validity of an Electronic Signature

The intention behind placing an electronic signature on any document is to produce specific legal effects. This signature enables the identity of the signatory to be determined and their capacity and powers to be ascertained. Furthermore, signing the document constitutes the signatories' acknowledgement and acceptance of its contents.

If legal scholarship and the judiciary have affirmed that the traditional handwritten signature produces these effects[31], the question that must be addressed is: What conditions must be satisfied by an electronic signature to produce the same effects as a traditional signature?

Previously, evidence laws required certain formal requirements alongside substantive requirements. Signatures were limited to paper documents by means of signing, stamping or fingerprinting. This meant that any other form would have no legal effect[32]. However, given the importance of electronic transactions in contemporary times, the growth of e-commerce and the emergence of new concepts such as e-government, legislators in different countries have enacted laws recognising electronic signatures, but only subject to specific substantive conditions.

Among these is what is stated in Article 26 of Regulation No. 2014/910, issued by the European Parliament and the Council on 23 July 2014[33], concerning electronic signatures. It provides that an electronic signature must satisfy the following conditions:

The signature must be linked to the signatory only.

It must uniquely identify the signatory and distinguish them from other persons.

The technical procedures used in relation to it must allow its origin/source to be verified.

It must also be linked to the information contained in the electronic document in such a way that any alteration affecting either the signature or the document's content can be detected.

In addition, on 13 March 2000, France issued a law regarding the development of the law of evidence and the adoption of electronic signatures and documents. This law provided a broad definition of the signature, focusing on its function and purpose rather than its form. Thus, Article 1316, paragraph four, excluded the phrase 'signing by handwriting' and replaced it with 'a signature issued by it', without specifying any particular formal requirement for the signature. Similarly, Article 1 of the French Decree No. 272/2001, issued on 30 March 2001, set out the conditions that must be met for an electronic signature. These can be summarised as follows:[34]

The signature must be distinctive, distinguishing its holder from others.

- The signatory must have sole control over the electronic medium.

- Any modification or alteration of the electronic instrument or signature data must be detectable.

Moreover, Article 6 of the UNCITRAL Model Law on Electronic Signatures (2001) provides that where the law requires a signature by a person, this requirement is deemed satisfied with respect to the data message if a reliable electronic signature is used for the purpose for which the data message was generated or communicated, taking into account all relevant circumstances, including any related agreement.

For the above purpose, an electronic signature shall be considered 'reliable' if the following conditions are met:

If the signature-creation data are linked to the signatory and to no other person in the context in which they are used, this requirement aims to prevent anyone other than the signatory from creating the electronic signature. Accordingly, the signature must be linked solely to the signatory, and not to any other person. Several forms of electronic signature satisfy this condition, including biometric signatures (based on the signatory's personal characteristics) and digital signatures that rely on a pair of keys (public and private).

- If the signature-creation data are subject to the control of the signatory alone at the time of signing: This condition requires that the authenticated electronic signature-creation instruments be under the control of the signatory alone, such as the private key in a digital signature being under the control of the person using that signature. The result is that the signatory cannot deny the signature or the legal effects arising from it.

- If any change to the electronic signature occurring after signing can be detected.

If the purpose of legally detecting the signature is to ensure the integrity of the information to which the signature relates and any change made to that information after signing is capable of being detected, this requirement aims to guarantee the integrity of the signed information. To this end, there must be a close link between the electronic signature and the signed information. Any amendment to the document after signing must entail a corresponding change to the electronic signature, and vice versa. Failure to satisfy this condition may allow someone to alter the electronic signature, transfer it from one record to another, or tamper with the signed information by deleting, adding to, or modifying it.

The position of the Algerian legislator

The Algerian legislator was clearly influenced by the European framework set out in Regulation No. 2014/910, which repealed the 1999[35] European Directive on electronic signatures. They were also influenced by the rules and provisions introduced by the UNCITRAL Model Law on Electronic Signatures (2001)[36]. In this context, the legislator distinguished between two types of electronic signature: a simple electronic signature, which is not based on accredited certification attesting to its validity; and a

qualified (advanced) or ‘described’ electronic signature, which is issued using a secure signature-creation device and is based on a certificate.

In this regard, Article 7 of Law No. 04-15, which set out the general rules relating to electronic signatures and certification (and has since been repealed), states that an electronic signature is one that meets certain conditions, namely:

1. It must be created on the basis of a qualified electronic certification certificate. This certificate is an electronic document that establishes a link between the electronic signature verification data and the signatory[37].

2. It must be linked to the signatory and no one else. This means that no one else can create the same electronic signature. Therefore, the qualified electronic signature is linked to the signatory alone. A signatory is defined as any natural person who possesses the electronic signature creation data and acts either on their own behalf or on behalf of a natural or legal person they represent (Article 2, paragraph two, of the same law).

3. It must enable the identification of the signatory, i.e. it must identify the signatory alone, to the exclusion of others.

4. It must be created using a secure mechanism dedicated to creating the electronic signature. Such a mechanism is a device or information system specially prepared to implement the creation of the electronic signature (Article 2, paragraph four of the same law).

5. It must be created by means under the signatory’s exclusive control: this condition requires the qualified electronic signature creation instruments to be under the signatory’s exclusive control. For example, the private encryption key in a digital signature must be under the signatory’s control only.

6. It must be linked to the relevant data, so that any subsequent changes can be detected. This means that there must be a close link between the signature and the information signed, so that any modifications affecting either the signature or the document content can be detected.

These conditions are emphasised by the Algerian legislator in Article 4 of the new law No. 26-02.

From the foregoing and the presentation of various legal texts, it can be concluded that most legislation has tended to equate electronic signatures with handwritten signatures provided they satisfy the relevant legal requirements. In that case, it can produce the same effects as the traditional signature and enjoy the same legal evidentiary force, provided certain conditions are met to make it a reliable, qualified or protected signature. This will become clearer in the next section.

Chapter Two: The Evidentiary Value of Electronic Signatures in Proof under the Provisions of Law No. 26-02

The recognition of the legal evidentiary value of electronic signatures hinges on two fundamental issues:

1. The role played by the electronic signature — in other words, whether an electronic signature can perform the same functions as a traditional signature.

2. The security and trust that must be provided by an electronic signature, and the technical accuracy of the signature.

As electronic signatures are a legal fact that cannot be ignored, it is necessary to address these issues in order to understand this modern technical instrument and avoid undermining trust in transactions involving electronic signatures, especially in civil transactions.

The first requirement: Functions of the Electronic Signature

In general, the role of an electronic signature is defined by three core functions:[38]

1. it verifies the identity of the signatory.

2. It expresses the signatory’s intent.

3. Thirdly, the signature indicates the presence of its holder, i.e. the signatory.

In light of these functions, we will attempt to ascertain the extent to which electronic signatures fulfil them, so that they may obtain full legal evidentiary value.

First function: Distinguishing the identity of the signatory

This means that the signature on the document must be attributed to a specific person. Examining the electronic signature reveals that it performs the same role using codes, numbers, letters or other indicators that reflect the signatory’s identity and distinguish them from others[39].

This is what most laws and legislation related to electronic signatures have adopted. This applies whether under Regulation No. 2014/910, the UNCITRAL Model Law on Electronic Signatures (2001), or the laws of various states concerning electronic signatures, including Algeria’s Law No. 04-15. These laws expressly require that for an electronic signature to have full evidentiary value, it must be linked to the signatory alone and allow their identity to be determined. Thus, the signatory’s identity is deemed guaranteed as soon as the electronic signature exists. This is the objective of adopting signatures in general and electronic signatures in particular.

Second function: Expressing the Will of the Signatory

This function involves verifying that the signatory is satisfied with and accepts the obligation set out in the legal act, and acknowledges that act. With respect to an electronic signature, the signatory's consent and acceptance of the obligation can be assumed once the electronic signature has been added to the data in the electronic documents. This is particularly true when the electronic signature takes the form of secret numbers or specific codes that are kept in the possession of the person who holds them and which no one else knows.

If those numbers are used, i.e. if the holder signs with them, the mere act of signing indicates agreement with the signed data and information, and that the signatory intends to be bound by it.

This occurs in practice when using electronic payment cards, which are among the most important real-world applications of electronic signatures. In such cases, the bank card holder expresses their clear intention by means of the electronic signature encoded in particular numbers, symbols or a specific cipher when dealing with an automated teller machine. The cardholder then instructs the machine to withdraw the desired amount. This process as a whole is considered to be the holder's consent and acceptance of the electronic document's contents.

Thus, the fundamental objective of signing the document is achieved: verifying its legal validity and confirming the signatory's satisfaction with its legal content.

Third function: The signature as proof of the signatory's presence

This function aligns perfectly with the nature of the traditional signature, which requires the physical presence of the signatory or a representative acting on their behalf. However, the concept of physical presence cannot be applied to electronic signatures. An electronic signature is essentially a modern means devised for use in distance contracting. This means that the parties do not need to be physically present at the same time and place when the legal act is concluded. Otherwise, recourse to an electronic signature would not be necessary.

Nevertheless, from a practical standpoint, nothing prevents this requirement from being met. This is exemplified by cases where clients enter secret codes themselves. In such cases, entering the code amounts to the client's signature, serving as evidence that they were personally present when the signing occurred.

Conclusion regarding the evidentiary value of electronic signatures:

In light of the foregoing presentation of these functions, we conclude that an electronic signature can fulfil the same legal requirements as a traditional signature. Accordingly, it has the same legal evidentiary force as an ordinary signature.

This has led to legal provisions being enacted in most laws governing electronic signatures, whether at the level of international organisations (e.g. the 2001 UNCITRAL Model Law), European directives or individual states, ensuring the principle of equivalence between electronic and traditional signatures in terms of the legal evidentiary value accorded to signatures carried out on paper media, but subject to certain conditions.

These laws distinguish between two types of electronic signature:

1. Simple electronic signature: not based on a trusted certification service or an approved certificate confirming its validity.

2. Advanced electronic signature:[40] issued using one of the secure signature-creation means or devices and based on a certification service. To be valid, an advanced electronic signature must satisfy a set of requirements, which can be summarised as follows:

- It must be intended to prove the identity of the signing party.

- The signature must be created using special means under the signatory's control.

- It must be linked to the associated data in such a way that any subsequent changes can be detected[41].

Evidentiary effects

The advanced electronic signature is considered equivalent to a traditional signature in its own right. It enjoys full legal evidentiary force whenever all the required conditions are met[42].

In contrast, the party seeking to rely on a simple electronic signature must provide evidence to the court regarding the reliability of the technical means used to create and issue it. The court has broad discretionary authority to determine the value of electronic signatures in evidence, relying on expert opinion.

Limits on Challenging Its Validity

Regarding the foregoing, it should be noted that the effectiveness of a simple electronic signature may never be invalidated or rejected as evidence in court on the grounds of its electronic form.

- its electronic form;

- it does not rely on an advanced electronic certificate;

- it was not created using a secure electronic signature creation mechanism.

From the foregoing, we infer that various legislations, including that of Algeria, tend to equate electronic signatures with traditional handwritten signatures, granting them the same legal evidentiary force in terms of proof. However, this legal force is not absolute; it is only granted to electronic signatures that satisfy specific conditions that render them reliable. Additionally, where duality exists between two electronic signatures — one simple and the other advanced — the latter prevails due to its security features[43].

While the electronic signature does not correspond to the traditional one in terms of form, it does so in terms of function, purpose and legal evidentiary force, subject to certain conditions. The essential difference between the two remains in the means used — namely, that the electronic signature is created using electronic media.

Second Requirement: Security and confidence must be ensured in the electronic signature.

Granting legal evidentiary force to electronic signatures is closely linked to the level of security they provide in transactions between interested parties. Thus, the level of security achieved must be such that the law can confer trust and legal evidentiary force upon it. In other words, trust in electronic signatures concerns the extent to which they comply with the technical conditions required by law. This relates to the electronic certification and authentication of the signature in accordance with the specific legal procedures established in this field.

Conclusion:

The tremendous development witnessed in the information and communications technology sectors, and the remarkable integration that occurred between them, clearly had a positive impact in bringing about the information revolution and consolidating e-commerce features. This represented a qualitative and civilisational leap in the lives of individuals and states.

Currently, various sectors primarily rely on information systems to perform their activities due to their speed and accuracy in collecting information. They also rely on electronic means and technologies. This study attempted to address the most significant problem that may confront electronic transactions — namely, the issue of proof — by defining the concept of the electronic signature and discussing its evidentiary value in proving civil transactions. The most important finding is that the electronic signature is a genuine alternative to the handwritten signature and resolves the issue of proving civil electronic transactions. Provided that it meets the required legal conditions, it enjoys the same legal evidentiary force in proving civil transactions as the traditional signature. Furthermore, electronic signatures provide greater security than traditional signatures because they substantially rely on encryption technology, meaning only the owner has knowledge of them.

The most important recommendations to include in the conclusion of this study are:

E-commerce has become a tangible reality that cannot be ignored. This requires the establishment of mechanisms and measures to create an appropriate environment for e-commerce, as well as the formulation of a legal framework to regulate electronic transactions. The aim is to promote and develop electronic exchanges, particularly civil transactions. The enactment of Law No. 18-05 on E-Commerce by the Algerian legislator may be considered a positive step towards consolidating this approach.

It provides the necessary technical and technological means to generalise the use of electronic signature systems at all levels.

The Algerian legislator has taken a further appropriate step by enacting Law No. 04-15 on Electronic Signature and Electronic Certification in an attempt to keep pace with global developments in this field. Various implementing regulations have also been issued to complete its implementation. However, bodies or authorities responsible for electronic certification still need to be established in order to enhance the credibility of electronic signatures and prevent their manipulation.

References:

First: Legal Texts

Law No. 04-15 dated 11 Rabiʿ al-Thani 1436 AH (corresponding to 1 February 2015) establishing the general rules relating to electronic signature and electronic certification (Official Gazette No. 06, published on 20 February 2015, repealed).

Law No. 26-02 dated 17 February 2026 establishing the general rules relating to trust services for electronic transactions and electronic identification (Official Gazette No. 14, published on 18 February 2026).

Executive Decree No. 07-162 dated 30 May 2007 amending and supplementing Executive Decree No. 01-123 of 9 May 2001 relating to the operating system applicable to each type of network, including wireless and electrical networks, and to various wired and wireless telecommunications services (Official Gazette No. 37, published on 7 June 2007).

UNCITRAL Model Law on Electronic Signatures (2001).

Law No. 2000-230 of 13 March 2000 on the adaptation of the law of evidence to information technologies and relating to electronic signature (Official Journal No. 62, 14 March 2000).

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, and repealing Directive 1999/93/EC (published in the Official Journal of the European Union on 28 August 2014).

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures (Official Journal of the European Communities, L 13, pp. 12–20, 19 January 2000).

Second: Books and Research Studies

Lazhar Ben Saïd, The Legal Framework of Electronic Commerce Contracts, Houma Publishing, Printing and Distribution House, Algeria, n.d. [no edition stated], 2012.

Alaa Muhammad Nusayrat, The Evidentiary Value of the Electronic Signature: A Comparative Study, Published Master's Thesis, Dar Al-Thaqafa for Publishing and Distribution, Jordan, 1st ed., 2005.

Wael Anwar Bandak, Electronic Signature Law: UNCITRAL Rules and Their Guide, Al-Wafaa Legal Library, Egypt, 1st ed., 2009.

Nidal Ismail Barham, Provisions Governing Electronic Commerce Contracts, Dar Al-Thaqafa for Publishing and Distribution, Jordan, 1st ed., 2005.

Amir Faraj Youssef, Electronic Signature, University Publications House, Egypt, n.d. , 2008.

Abdel Fattah Bayoumi Hegazy, Electronic Signature in Comparative Legal Systems, University Thought House, Egypt, 1st ed., 2005.

Najwa Abu Hiba, "Electronic Signature: Its Definition and Evidentiary Value," research paper presented at the Conference on Electronic Banking between Sharia and Law, held from 10–12 May 2003, College of Sharia and Law, United Arab Emirates University, and Dubai Chamber of Commerce and Industry, Vol. 1.

Zahra, Muhammad Al-Mursi, 'The Evidentiary Value of the Electronic Signature', in Legal Aspects Arising from the Use of Computers in Banks, 2nd ed., Cairo: Union of Arab Banks, 1999.

Ibrahim Al-Desouki Abu Al-Leil, 'Documentation of Electronic Transactions and the Liability of the Certifying Authority towards the Injured Third Party', research paper presented at the 'Conference on Electronic Banking between Sharia and Law', held by the College of Sharia and Law and the Dubai Chamber of Commerce and Industry in the United Arab Emirates from 10–12 May 2003, Vol. 5.

Najwa Abu Hiba, Electronic Signature: Its Evidentiary Value', Dar Al-Nahda Al-Arabiya, Cairo, Egypt, n.d., 2004.

Ayed Rachid Al-Marri, 'The Evidentiary Value of Modern Technology in Proving Commercial Contracts', PhD dissertation, Faculty of Law, Cairo University, 1998.

Hassan Abdel Basit Gomei, 'Proof of Legal Acts Concluded via the Internet', Dar Al-Nahda Al-Arabiya, Egypt, 2000.

Atef Abdel Hamid Hassan, Electronic Signature: Its Concept, Forms and Evidentiary Value within the Scope of Civil Transactions', Dar Al-Nahda Al-Arabiya, Egypt, no edition stated, 2008.

Virginie Etienne, 'The Development of the Electronic Signature', Université Paris Nord 13.

Notes

[1] - The specificity of the electronic contract lies in the electronic aspect of this contract, or in the means by which it is concluded. Various definitions have been given of this contract, including doctrinal and legislative definitions, as well as the definition contained in the United Nations Model Law. In general, however, it may be defined as: "A contract concluded by means of one or more electronic methods, whether wholly or partially, provided that such methods generate the interaction required to complete the contract between its parties and give rise to obligations incumbent upon them." For further details on this contract, see: Lazhar Ben Saïd, The Legal Regime of Electronic Commerce Contracts, Dar Houma for Printing, Publishing and Distribution, Algeria, n.p., 2012, p. 43 et seq.

[2] - Legal systems have differed in determining the principles of evidence. Some legal systems have adopted the principle of freedom of evidence, whereas others have adopted the principle of restricted evidence.

[3] - Law No. 04-15 of 11 Rabi' al-Thani 1436 AH, corresponding to February 1, 2015, establishing the general rules relating to electronic signatures and electronic certification, Official Gazette, No. 06, issued on February 20, 2015. Repealed.

[4] - Law No. 26-02 of February 17, 2026, establishing the general rules relating to trust services for electronic transactions and electronic identification, Official Gazette, No. 14, issued on February 18, 2026.

[5] - Alaa Muhammad Nusairat, The Evidentiary Value of the Electronic Signature: A Comparative Study, published Master's thesis, Dar Al-Thaqafa for Publishing and Distribution, Jordan, 1st ed., 2005, p. 15.

[6] - UNCITRAL Model Law on Electronic Signatures, 2001.

[7] - The other organizations that attempted to define the electronic signature were largely influenced by the definition provided by the UNCITRAL Model Law on Electronic Signatures.

[8] - See the commentary on this provision in: Wael Anwar Bandak, The Electronic Signature Law: UNCITRAL Rules and Their Legislative Guide, Al-Wafaa Legal Library, Egypt, 1st ed., 2009, p. 85.

[9] - Nidal Ismail Barham, The Rules Governing Electronic Commerce Contracts, Dar Al-Thaqafa for Publishing and Distribution, Jordan, 1st ed., 2005, p. 170.

[10] - See in this regard: Alaa Muhammad Nusairat, op. cit., p. 23; Nidal Ismail Barham, op. cit., pp. 170–171.

[11] - Law No. 2000-230 of March 13, 2000, on the Adaptation of the Law of Evidence to Information Technologies and Relating to Electronic Signatures, Official Journal, No. 62, March 14, 2000.

[12] - The following observations may be made concerning the French legislator's definition of the electronic signature: First – It focused on the function of the signature and, consequently, left the scope broad enough to encompass every signature that fulfills its purposes. Second – It did not focus on any particular method for defining the electronic signature. Third – It required the method by which the signature is created to be reliable, that is, to possess a sufficient degree of accuracy. Fourth – It required the signature to be connected to the document to which it relates.

[13] - Law No. 04-15, repealed by Law No. 26-02 establishing the rules relating to trust services for electronic transactions and electronic identification, op. cit.

[14] - Abd al-Fattah Bayoumi Hegazy, The Electronic Signature in Comparative Legal Systems, Dar Al-Fikr Al-Jami'i, Egypt, 1st ed., 2005, p. 66.

[15] - Najwa Abu Hayba, The Electronic Signature: Its Definition and Its Evidentiary Value, paper presented at the Conference on Electronic Banking Transactions between Sharia and Law, held from May 10–12, 2003, Faculty of Sharia and Law, United Arab Emirates University, and Dubai Chamber of Commerce and Industry, Vol. 1, p. 442.

[16] - Muhammad al-Mursi Zahra, The Evidentiary Value of the Electronic Signature, paper published in The Legal Aspects Arising from the Use of Computers in Banks, Union of Arab Banks, Cairo, Egypt, 2nd ed., 1999, p. 163.

[17] - Nidal Ismail Barham, op. cit., p. 172.

[18] - Muhammad al-Mursi Zahra, op. cit., p. 167.

[19] - Ibrahim al-Dusuqi Abu al-Layl, Authentication of Electronic Transactions and the Liability of the Certifying Authority toward the Injured Third Party, paper presented at the Conference on Electronic Banking Transactions between Sharia and Law, held in the United Arab Emirates by the Faculty of Sharia and Law and the Dubai Chamber of Commerce and Industry from May 10–12, 2003, Vol. 5, p. 1854.

[20] - Amir Faraj Yusuf, The Electronic Signature, op. cit., p. 19.

[21] - Najwa Abu Hayba, The Electronic Signature: Its Evidentiary Value, Dar Al-Nahda Al-Arabiya, Cairo, Egypt, n.p., 2004, p. 70.

[22] - Amir Faraj Yusuf, The Electronic Signature, op. cit., p. 19; Nidal Ismail Barham, op. cit., p. 173.

[23] - Najwa Abu Hayba, The Electronic Signature: Its Evidentiary Value, op. cit., p. 66.

[24] - Alaa Muhammad Nusairat, op. cit., pp. 39–40; Nidal Ismail Barham, op. cit., pp. 173–174.

[25] - Virginie Etienne, The Development of the Electronic Signature, Université Paris Nord 13, p. 15.

[26] - Ayed Rashid Al-Marri, The Evidentiary Value of Modern Technology in Proving Commercial Contracts, PhD dissertation, Cairo University, Faculty of Law, 1998, p. 97.

[27] - Hassan Abd al-Basit Jumai'i, Proof of Legal Acts Concluded through the Internet, Dar Al-Nahda Al-Arabiya, Egypt, 2000, p. 42; Nidal Ismail Barham, op. cit., p. 174.

[28] - Ayed Rashid Al-Marri, op. cit., p. 112.

[29] - Alaa Muhammad Nusairat, op. cit., pp. 34–35.

[30] - Ayed Rashid Al-Marri, op. cit., p. 113; Alaa Muhammad Nusairat, op. cit., p. 35; Nidal Ismail Barham, op. cit., p. 175.

[31] - Saeed Al-Sayyid Qandil, The Electronic Signature, op. cit., p. 48.

[32] - Nidal Ismail Barham, op. cit., p. 176.

[33] - Regulation No. 910/2014 of the European Parliament and of the Council of July 23, 2014, on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, was published in the Official Journal of the European Union on August 28, 2014.

[34] - Article 1 – For the purposes of this Decree, the following definitions shall apply: …… 2 – A secure electronic signature is an electronic signature that, in addition, satisfies the following requirements: it is uniquely linked to the signatory; it is created by means that the signatory can maintain under his or her exclusive control; and it guarantees, with the document to which it is attached, a link such that any subsequent modification of the document can be detected.

[35] - Directive 1999/93/EC of the European Parliament and of the Council of December 13, 1999, on a Community framework for electronic signatures, Official Journal of the European Communities, L 13/12–20, January 19, 2000.

[36] - This is the same approach adopted by the Egyptian legislator in Article 15 of Law No. 15 of 2004 regulating electronic signatures and establishing the Information Technology Industry Development Agency, op. cit.

[37] - Article 2, paragraph 7, of Law No. 04-15, op. cit.

[38] - Atef Abd al-Hamid Hassan, The Electronic Signature: Its Concept, Forms, and Evidentiary Value in the Context of Civil Transactions, Dar Al-Nahda Al-Arabiya, Egypt, n.p., 2008, p. 78 et seq.

[39] - Najwa Abu Hayba, The Electronic Signature: Its Evidentiary Value, op. cit., p. 107.

[40] - Several terms have been used to designate this type of electronic signature, which requires the fulfillment of certain conditions. The Algerian legislator uses the term "qualified electronic signature," whereas the European Directive uses the term "advanced electronic signature" (la signature électronique avancée) (Article 3, paragraph 11, of European Regulation No. 910/2014), while the UNCITRAL Model Law uses the term "reliable electronic signature" (Article 6, paragraph 3). All of these terms convey essentially the same meaning.

[41] - Article 7 of Law No. 26-02 establishing the rules relating to trust services for electronic transactions and electronic identification.

[42] - Article 16 of Law No. 26-02, op. cit.

[43] - Said Al-Sayyid Qandil, op. cit., p. 55.