

Electronic Contract in Algerian Civil Law.

العقد الإلكتروني في القانون المدني الجزائري

Berkane Fadhila*

University of Yahya Fares – Medea, Faculty of Law and Political Sciences,

Laboratory for Sovereignty and Globalization Studies

berkane.fadhila@univ-medea.dz

Date of Submission 02-04-2026 Date of Final Acceptance 18-07-2026 Date of Publication September 2026

Abstract:

This study examines the legal framework of electronic contracts in the context of digital transformation, with a particular focus on Algerian legislation compared to comparative laws. The research highlights that the digital revolution has necessitated a reconsideration of traditional contracting rules, leading to the emergence of electronic contracts as a fundamental tool in the digital economy. The study explores the concept and characteristics of electronic contracts, emphasizing their remote nature and commercial-consumer character, while addressing the evidentiary challenges through the principle of functional equivalence between electronic and paper writing. It discusses the conditions for accepting electronic writing as evidence, primarily verifying the signatory's identity and ensuring content integrity. The research analyzes various types of electronic signatures (biometric, digital, coded, electronic pen) and compares them with ordinary signatures in terms of form, medium, and function. It concludes that the Algerian legislator has successfully established a legal framework for electronic contracts through Laws 15-04 and 18-05, yet the current framework requires continuous development to keep pace with technological advancements and cross-border challenges.

Keywords: Electronic Contract, Digital Transformation, Electronic Evidence, Electronic Signature, Electronic Authentication.

الملخص:

يتناول هذا البحث الإطار القانوني للعقد الإلكتروني في سياق التحول الرقمي، مع تركيز خاص على التشريع الجزائري مقارنة بالقوانين المقارنة. يبرز البحث أن الثورة الرقمية فرضت إعادة النظر في القواعد التقليدية للتعاقد، مما أدى إلى ظهور العقد الإلكتروني كأداة أساسية في الاقتصاد الرقمي. يستعرض البحث مفهوم العقد الإلكتروني وخصائصه، مبرزاً طابعه التعاقدي عن بُعد وطبيعته الاستهلاكية التجارية، كما يعالج الإشكاليات الإثباتية من خلال مبدأ التكافؤ الوظيفي بين الكتابة الورقية والإلكترونية. ويناقش البحث الشروط الواجب توافرها لقبول الكتابة الإلكترونية كدليل، وعلى رأسها التحقق من هوية الموقع وضمان سلامة المحتوى. كما يُحلل البحث أنواع التوقيع الإلكتروني المختلفة (البيومتري، الرقمي، المشفر، بالقلم الإلكتروني) ويقارنها بالتوقيع العادي من حيث الشكل والوسيط والوظيفة. ويخلص البحث إلى أن المشرع الجزائري نجح في وضع إطار قانوني للعقد الإلكتروني من خلال القانونين 04/15 و 05/18، إلا أن هذا الإطار يظل بحاجة إلى تطوير مستمر لمواكبة التطورات التقنية المتسارعة والتحديات العابرة للحدود.

الكلمات المفتاحية: العقد الإلكتروني، التحول الرقمي، الإثبات الإلكتروني، التوقيع الإلكتروني، التصديق الإلكتروني.

* Corresponding Author: BERKANE Fadhila

Introduction:

The digital revolution and the rapid transformation in information and communication technology have produced a new legal reality that has forced various legislative systems to reconsider the traditional rules governing contractual relationships. Contracting is no longer confined to the traditional framework based on physical meetings between parties and the exchange of paper documents. Instead, it now often occurs through modern electronic media, relying on digital communication networks and information systems, which has given rise to what is known as electronic contract.

Electronic contract is considered one of the most prominent manifestations of the digital transformation the world is witnessing today, as it constitutes the legal basis for e-commerce, digital services, e-government, and the digital economy in general. This type of contract has contributed to facilitating and expediting transactions, overcoming temporal and spatial constraints, and reducing costs, making it an indispensable tool in the context of economic globalization.

However, this development, despite its positives, has raised complex legal issues related to the concept of the contract itself, its elements, methods of expressing will, evidentiary value, electronic signatures, as well as the issue of protecting the e-consumer, and determining the applicable law and jurisdictional competence given the cross-border nature that characterizes the digital environment. The complexity of these issues has increased with the acceleration of digital transformation projects adopted by countries, including Algeria, as part of modernizing administration and developing the national economy.

The Algerian legislator has recognized the importance of keeping pace with these transformations, working to integrate modern technologies into the legal system through enacting special legislative texts aimed at regulating electronic transactions and bestowing legal validity on digital media. Law No. 15-04 concerning electronic signatures and certification, and Law No. 18-05 concerning e-commerce are among the most prominent texts that form the legal framework for electronic contracts in Algeria, in clear harmony with the requirements of digital transformation.

In the same context, the international arena has witnessed extensive legislative efforts to regulate the electronic contract, most notably the Model Laws issued by the United Nations Commission on International Trade Law¹ (UNCITRAL², in addition to European legislation, particularly directives concerning distance contracting and consumer protection in the digital environment. These texts have served as a fundamental reference for many national legislations, including Algerian legislation.

Based on the above, the central problematic of this study emerges in the following main question:

To what extent has Algerian legislation succeeded in regulating the electronic contract and keeping pace with the digital transformation, compared to international legislations, while ensuring legal security and protecting the parties to the contractual relationship?

This study aims to:

1. Highlight the conceptual and legal framework of the electronic contract in Algerian legislation.
2. Analyze the Algerian legal texts regulating electronic contracting.
3. Compare Algerian legislation with relevant international legislations.
4. Clarify the role of electronic contracts in the success of digital transformation projects.

5. Evaluate the effectiveness of the current legal framework and propose prospects for its development.

Research Methods:

This study adopts a descriptive approach to investigate electronic contract laws within Jordanian legislation. It aims to provide a detailed exploration of electronic contracts, including their formulation, configuration, and associated legal obligations. The study relies on secondary descriptive data gathered from various sources such as books, websites, articles, and official sources. Simple content analysis technique is employed to analyse the collected data, with the main findings presented in the conclusion.

Chapter One: The Nature of the Electronic Contract:

The digital transformation has brought about a profound revolution in the methods of concluding legal transactions, as contractual relationships have shifted from the traditional framework based on physical presence and paper documents to an electronic space relying on modern communication technologies and information systems. This new reality has forced legal thought and national and international legislation to absorb this transformation by developing traditional legal concepts, foremost among them the concept of the contract.

In this context, the electronic contract has emerged as one of the most important tools of the digital economy, becoming the legal framework under which most electronic transactions are concluded, whether in the fields of commerce, services, or e-government. However, this development has produced precise legal issues related to defining the nature of the electronic contract and distinguishing it from other contracts associated with the digital environment, which necessitates an in-depth study of its concept and boundaries.

Accordingly, this chapter is dedicated to defining the nature of the electronic contract by studying its concept in comparative laws in the first section. The second section addresses the characteristics of the electronic contract, while the third section establishes the distinctive basis that sets the electronic contract apart from other contracts.

Section One: The Concept of the Electronic Contract:

Accordingly, the first section is dedicated to the concept of the electronic contract, with (A) defining the electronic contract, and (B) addressing its definition in comparative laws.

A- Definition of the Electronic Contract:

Definition of e-commerce in general and e-contracts, in particular, was one of the things that sparked controversy and had differing views. The reason for such disagreement maybe is probably due to the complexity of this type of commerce and the diversity of contracts involved, which led to different concepts and definitions. And whereas e-contract is a form of a distance contract, it was defined by the Article 2 of the Directive of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts as: “any contract concerning goods or services concluded between a supplier and a consumer under an organized distance sales or service provision scheme run by the supplier, who, for the purpose of the contract, makes exclusive use of one or more means of distance communication up to and including the moment at which the contract is concluded”. While Article 2 of the Electronic Transactions and Commerce Law No. 16 of 2010, defined electronic transaction as: “any deal, contract or agreement concluded or performed, in whole or in part, through electronic communications”.

A part of legal jurisprudence based its definition of e-contract on the capacity and characteristics of the contracting parties and defined it as: "The performance of some or all business-to business or business-to-consumer transactions for goods and services through³ information and communication technology". E-contract has several characteristics, the most important of which is that it is a distance contract. The essential feature of the e-contract is that it is concluded between two contracting parties do not present in an actual contracting setting but rather concluded remotely⁴ through different technological means via a virtual or constructive contracting session. E-contract is also characterized by commercial nature, as well as consumer nature as it is often concluded between a merchant and a consumer, therefore it is a consumption contract. In addition, one of the distinguishing characteristics of the e-contract is that it is a bargaining contract. Mere agreement of the contracting party to the pre-set conditions is not the end of it, but rather he has the right to move from one site or offer to another and choose and leave whatever he wants. Therefore, consensuality is prevailing in e-contracts, not adhesion.⁵

B- Definition of the Electronic Contract in Comparative Laws:

National legislations, in the context of keeping pace with digital transformation, have sought to regulate electronic contracts and grant them legitimacy, either by explicitly defining them or by recognizing the means of their conclusion and proof. The study of comparative laws shows diversity in legislative style with unity in purpose.

1- Tunisian Legislation:

The Tunisian legislator regulated electronic transactions under Law No. 83 of 2000 concerning exchanges and electronic commerce, where it recognized the validity of electronically concluded contracts, and stipulated that the exchange of electronic messages produces the same legal effects produced by paper instruments⁶. It is noted that the Tunisian legislator did not provide a direct definition of the electronic contract, but adopted a functional approach based on recognizing electronic means as a legitimate contracting tool.

2- Jordanian Legislation:

In the Jordanian Electronic Transactions Law No. 15 of 2015, Article 2 defines "transactions" as encompassing any action executed among one or more parties, leading to the creation of an obligation on one party or reciprocal obligations among multiple parties, irrespective of whether the action pertains to commercial, civil, or governmental affairs. Moreover, the same provision defines an "electronic document" as a document formulated, signed, and exchanged electronically⁷.

3- Egyptian Legislation:

The Egyptian legislator adopted the Electronic Signature Law No. 15 of 2004, which bestowed legal validity on the electronic signature and instrument, which directly reflects on electronic contracts as electronic instruments producing legal effects⁸. It is noted that Egyptian regulation focused more on evidence than definition, reflecting its concern for securing trust in digital transactions.

4- French Legislation:

The French legislator enshrined the explicit recognition of the electronic contract by amending the Civil Code, particularly Article 1127-1, which affirmed the validity of electronically concluded contracts, and confirmed the principle of equality between electronic writing and paper writing⁹. French legislation is considered one of the most developed in this field, due to its adoption of a clear definition consistent with European directives.

Through this comparison, comparative legislations agree on recognizing the electronic contract, with differences in drafting style between explicit definition and implicit regulation.

Section Two: The Characteristics of an Electronic Contract

An Electronic Contract is Formed Remotely. This means the parties are not physically present in the same location when concluding the contract, exchanging offers and acceptances electronically over the internet. This type of agreement is often referred to as a "cyber forum" because it is formed between virtually absent parties. Through data exchange via electronic intermediaries, there is an opportunity to establish and verify the identities of the contracting parties. The international nature of electronic commercial transactions introduces various legal issues, such as the applicable law and the competent court for disputes. However, an electronic contract may still be considered domestic if it lacks international elements.

A-Electronic Contract is Characterized Using Electronic Means to Conclude the Contract over the Internet:

This feature is a key aspect of the specificity of electronic contracts. Although electronic contracts align with the general provisions of ordinary contracts regarding the place of commitment and legal effects, they differ in requiring electronic tools for negotiations, communication, and the exchange of deliberate expressions through the internet. Consequently, electronic contracts cannot be formed without these methods, which facilitate the convergence of the contracting parties' intentions. The electronic environment, therefore, is both technically and legally conducive to the formation of electronic contracts.

B-Often Electronic Contracts Exhibit a Commercial Consumer Nature:

These contracts are commonly referred to as electronic commerce contracts because their nature, particularly in the online domain, is closely tied to electronic commerce activities. The concept of electronic commerce is indirectly defined in Article 1 of the United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce, encompassing all commercial activities and related issues conducted, sent, or received through electronic means or similar methods.

An electronic seller typically operates an electronic platform—a dedicated online space accessible at any time—where they display content related to their business activities. In this context, users, whether natural or legal persons, must act in good faith, with dealings conducted transparently and clearly. In certain jurisdictions, such as under Article 12/8 of the French Consumer Protection Law issued by Decree No. 741/2001, professionals or business entities are required to provide consumers with all relevant identifying information, such as the company name and nature of the business. This transparency is crucial to protect consumers from fraud or deception by the other party.¹⁰

Section Three: Electronic Contracts Distinctive Basis from Other Contracts

The electronic contract, or e-commerce contract, is not the sole contract formed within the digital environment, as there are other agreements entered into within this sphere, often interconnected with the electronic contract. We will now examine the distinguishing features that set the electronic contract apart from other contracts.

A-Distinguishing Between the Electronic Contract and the Contract Concluded by Phone:

Contracts can be oral or written, but when concluded via phone, they are typically oral due to geographical distance. This contrasts with electronic contracts, where the offer and acceptance are often in written form, electronically. Notably, this writing is electronic. However, oral agreements through technology (e.g., Skype, chat) are also possible. In e-commerce contracts, there is no traditional face-to-face meeting; the environment is virtual, without physical boundaries. Parties may be in different locations, even with a time difference between them. Contracting via phone involves parties present in terms of time but absent in terms of location, akin to remote contracts. In this sense, e-contracts are characterized by their virtual nature, unlike traditional contracts involving face-to-face meetings.

B-Distinguishing Between the Electronic Contract and Telex:

Telex, an instantaneous communication method, provides substantial verification assurances, ensuring addressee identity, as well as information confidentiality and security. Telex produces printed paper outputs on specialized machines, allowing for document preservation, albeit without the capability to transmit graphics, images, and signatures. Contracting via telex may share similarities with an electronic contract in its legal nature. However, a notable distinction lies in the fact that messages sent over the Internet or via email need not be printed for recipient comprehension. Such messages can incorporate images, audio files, or text.

C-Distinguishing Between the Electronic Contract and Television Contract:

In a television contract, there often exists a unilateral contract arrangement, devoid of direct interaction between the parties involved. The offer or¹¹ conveys their intent to contract either through telephone communication or by dispatching a message to a designated address specified by the accepting party, primarily aimed at distributing the offered products, goods, and marketing services. Conversely, electronic or smart contracts are distinguished by the interactive engagement between the contracting parties within a virtual contractual domain facilitated through the Internet or online platforms. Contracting via television typically involves both parties being present concurrently in terms of time, with no temporal gap between the offer and acceptance. This mode of contracting is conducted remotely due to the absence of physical proximity between the parties. There exists a potential similarity between electronic contracts and television-based contracts when contracting occurs through a website, presenting goods via images,

Enabling consumers to make informed decisions. Legal scholars posit that the principal distinction between internet-based contracting and television-based contracting lies in the manner of offer and acceptance. In internet contracting, both offer and acceptance occur through the same website, whereas in television contracting, an additional device is required to receive the acceptance.

Chapter Two: Proving Electronic Contract:

Section One: The Requirement for Written Evidence in Civil Proof:

Proof is the cornerstone of protecting civil rights, as a right has no value unless it can be proven before judiciary. The Algerian legislator has given special attention to written evidence, considering it the safest and most stable means of proving legal acts, due to its precision in determining the content of the obligation, continuity in its preservation, and the possibility of referring to it in the event of a dispute.

However, the rapid technological development and the resulting modern electronic means for concluding contracts and documenting transactions have forced a reconsideration of the traditional concept of writing, which was linked to the paper medium. Faced with this reality, the Algerian legislator found itself challenged to reconcile preserving the traditional rules of evidence with ensuring the absorption of digital transformation without compromising legal security.

From this standpoint, the legislator adopted the principle of functional equivalence between electronic writing and paper writing (A), while subjecting the former to strict conditions ensuring that it performs the same legal functions performed by traditional writing (B).

A- The Algerian Legislator's Principle of Functional Equivalence between Electronic Form Writing and Paper Writing:

The principle of functional equivalence represents the theoretical and legal foundation that allowed the integration of electronic writing into the civil evidence system. This principle is based on transcending the formal view of writing, and adopting an objective criterion focused on the legal function it achieves, regardless of the technical means used.

Functional equivalence means that electronic writing has the same legal value enjoyed by paper writing, provided it performs the same basic functions, namely proving the existence of the legal act, determining its content, and ensuring the possibility of attributing it to its author. Thus, the Algerian legislator did not make paper an essential condition for writing but considered it merely a traditional medium that carried writing in a specific historical period.

The Algerian legislator enshrined this principle by introducing explicit provisions recognizing writing in electronic form and granting it evidentiary value when legal conditions are met¹². This approach reflects a clear desire to keep pace with digital transformation, especially given the widespread use of electronic transactions in the civil and economic fields.

The principle of functional equivalence also achieves several legal objectives, including:

- Facilitating civil transactions by recognizing modern electronic means.
- Achieving legal security by subjecting electronic writing to the same functional standards as paper writing.
- Avoiding the legislative vacuum that may arise from adhering to the traditional concept of writing.

Therefore, this principle constitutes the general framework that allows accepting electronic writing as evidence, without compromising the rights of the parties or the integrity of legal transactions.

B- Conditions for Accepting Electronic Form Writing as Evidence:

Despite affirming the principle of functional equivalence, the Algerian legislator recognized that electronic writing involves technical and legal risks unknown to paper writing, which necessitated subjecting it to precise conditions aimed at ensuring its credibility and merit in evidence. The legislator limited these conditions to two fundamental elements, representing the essence of trust in written evidence.

1- The Ability to Verify the Identity of the Person Who Issued the Writing:

The condition of verifying the identity of the source of electronic writing is an essential condition for accepting it as evidence, as it is inconceivable to have a valid legal act without the

possibility of attributing it to a specific person¹³. This condition embodies an extension of the principle of consent, which is the basis of obligation in civil law.

This condition becomes even more important in the digital environment, where identity theft or the use of technical means to conceal the identity of the transactor is easy. Therefore, the Algerian legislator required the availability of technical means allowing verification of the identity of the person who issued the electronic writing, ensuring its attribution to them with certainty.

The electronic signature is the primary means of achieving this condition, as it allows linking the electronic instrument to its author legally and creates a presumption that the act originated from them, provided the legally prescribed conditions are met¹⁴. Thus, the electronic signature performs the same function performed by the handwritten signature on paper instruments.

2- That the Writing is Prepared and Preserved Under Conditions Ensuring its Integrity:

In addition to the identity condition, the Algerian legislator required that the electronic writing be prepared and preserved under technical conditions ensuring its integrity, i.e., its resistance to alteration or manipulation after its creation. The integrity of electronic writing means preserving its original content, with the possibility of referring to it at any time with the same characteristics with which it was created.

This condition compensates for the absence of the paper medium, which traditionally represented a material guarantee against forgery. It also aims to enhance trust in electronic instruments and ensure the continuity of their legal validity when presented as evidence before the civil judiciary.

Section Two: The Electronic Signature and its Comparison with the Ordinary Signature:

Information and communication technology opened wide horizons for individuals, resulting in the emergence of the internet as a huge network of interconnected computers worldwide.¹⁵ This enabled individual, despite differences in location, culture, and language, to communicate across the artificial boundaries between countries and peoples.¹⁶

The benefits of the internet were not limited to exchanging information, but it also turned into a means for concluding various types of contracts, which includes the electronic signature. We will discuss in this section the definition of the electronic signature¹⁷ and its conditions (A), as well as distinguishing between the electronic signature and the traditional signature (B).

A- Definition and Conditions of the Electronic Signature:

1- Definition of the Electronic Signature:

Some international organizations have addressed the definition of the electronic signature, including the United Nations Commission on International Trade Law (UNCITRAL) and the European Union. UNCITRAL issued a Model Law on Electronic Signatures approved on July 5, 2001.¹⁸ where it defined the electronic signature in Article 2 as:

"Data in electronic form which are attached to or logically associated with other electronic data, and which serve as a method of authentication."

It is noted that this definition did not specify the method by which the electronic signature is made, allowing each country to use the method it deems appropriate, whether symbols, signs,

numbers, or any reliable means. The definition also focuses on the functions of the electronic signature in identifying the signatory and expressing their agreement to the information contained.¹⁹

As for the European Union, it issued Directive 1999/93/EC on electronic signatures, where it defined the electronic signature in Article 2 as:

"Data in electronic form which are attached to or logically associated with other electronic data, and which serve as a method of authentication."²⁰

This definition addresses the electronic signature from a technical perspective, considering it a technological means that ensures security and confidentiality in the electronic message, so that no one other than the intended recipient can read it, and the sender cannot modify it.

The Algerian legislator stipulated the electronic signature in Law No. 15-04 dated April 10, 2015, which defines the general rules relating to electronic signatures and certification.²¹ Thus, the electronic signature is defined as:

"Data in electronic form, separate or logically linked to other electronic data, used as an authentication means."

Through the electronic signature, the identity of the signatory can be determined and authenticated, and their acceptance of the content of the writing in electronic form can be proven.

The electronic signature is anything placed on the electronic document, such as letters, numbers, symbols, signs, etc., allowing the identification of the signatory's personality and distinguishing them from others. The electronic signature may be with an electronic pen, digital signature, biometric signature, or electronic fingerprint.

2- Conditions of the Electronic Signature:

2.1- The electronic signature must be linked to the signatory and no one else:

The Algerian legislator, like many other legislations, affirmed that the electronic signature must be made by the signatory alone and no one else. The purpose of this is to ensure recognition of the signatory's will and consent to the content of the act. There must be a direct relationship between the signatory and the signature, so that the signature is used only by the person concerned, without allowing others to use it.

2.2- The signature must be sufficient to identify its owner:

This condition is considered self-evident, as the signature, regardless of its form, must be exclusive to its owner. The signature must be uniquely distinctive and linked to the signatory, allowing their identification.

2.3- It must be designed using a secure mechanism specific to creating the electronic signature:

This condition is fulfilled when the signature relies on a secure data system for creating the electronic signature. This system is considered secure if the following conditions are met:

- The unique character of the electronic signature creation data: The signature data must be unique and non-repeating.

- Confidentiality of the electronic signature creation data: The data must be protected so that they cannot be accessed except by the signatory.
- Non-infer ability or non-derivability of the electronic signature creation data: The data must be secured against any attempts to infer or deduce them.
- Protection of the electronic signature from forgery or imitation: There must be means to prevent any form of forgery or alteration.
- Not causing any damage to the content of the electronic instrument: The signature must ensure that the content of the electronic instrument to be signed is not changed.

2.4- Creation of the electronic signature by means specific to the signatory and under their sole control:

For the electronic signature to be effective, it must be created using tools under the control of the signatory.²² Among these tools is the private digital signature key. These tools must be protected so that no one else can access them. The key holder must ensure it is not leaked, and the tools for creating the signature system must be under their control.

2.5- The electronic signature must be linked to the data of the electronic instrument in a way that reveals any subsequent changes to this data:

The electronic instrument, including its private data and signature, is exposed to change during transmission due to third-party interference or technical malfunction. Therefore, the Algerian legislator required that the electronic signature be linked to the instrument in a way that ensures the detection of any subsequent changes.

The aim of this is to protect the electronic instrument and ensure the integrity of the information contained in it, as any modification of the data affects its validity as evidence, and this also applies to the evidentiary value of the electronic signature.

The process of examining the electronic signature data system is facilitated by the sender's public key, which allows the recipient to verify the integrity of the instrument. The recipient uses their program to create another summary of the electronic instrument, then compares this summary with the summary received. If they match, this means the electronic instrument is intact and has not been subject to any illegal interference.

The identity of the signatory can be recognized through what is known as the private key, which represents the pen in traditional signing. This key is supported by a password kept by the signatory alone, allowing them to access the private key.

As an example of this condition, signing with a password on ATM cards is a good example. When the cardholder enters their personal password into the ATM machine, the machine recognizes the password, allowing the person to access their account. Thus, these procedures are sufficient to indicate the user's identity, enabling them to perform the desired financial operations.

2.6- It must be created based on a qualified electronic certification certificate:

To ensure the integrity of electronic transactions, it is essential to verify the validity and integrity of the electronic signature through certification. The signature is certified by an authorized body or administration to verify the signature and grant a certification certificate. This procedure aims to prevent fraud or forgery crimes that may occur if the signature is altered or forged, negatively affecting the credibility of electronic transactions.

The purpose of this condition is to protect electronic transactions conducted over the internet, which is considered open to everyone, making the network vulnerable to hacking.

Returning to the position of the Algerian legislator, it gave special importance to this condition, granting independent administrative bodies, including the Regulatory Authority for Post and Electronic Communications, the authority to license certification service providers.

If a service provider issues authentication certificates before obtaining a license, this is considered a violation of the law. Consequently, the provider is subject to the penalties prescribed for violating the rules for licensing and regulating the work of certification service providers.

Article 72 of the Law concerning electronic signatures and certification also stipulates the penalties in this case, where imprisonment from one to three years, and a fine ranging from 200,000 DZD to 2,000,000 DZD, or one of these two penalties only, is imposed on anyone who provides electronic certification services to the public without a license, or any certification service provider who resumes or continues its activity despite the withdrawal of its license.

B- Comparison between the Ordinary Signature and the Electronic Signature:

1- In Terms of Form:

A signature is defined as any distinctive mark specific to the signatory, allowing their identity to be determined and recognized easily, thus showing their explicit will to consent to the contract. While the traditional signature is limited in form to specific images such as a signature and fingerprint, in addition to a seal impression in some legislations like Egyptian legislation, the electronic signature is not limited to specific images.

The electronic signature can take multiple forms, such as images, numbers, symbols, signs, or even sounds. The only condition is that this form has a unique character that allows distinguishing the signatory, determining their identity, and expressing their will to conclude the legal act and be bound by it.

2- In Terms of the Medium on Which it is Placed:

The traditional signature is usually placed on a physical medium, often paper. In contrast, the electronic signature is placed via an intangible electronic medium, giving it more flexibility in use.

3- In Terms of the Functions Performed by the Signature:

The traditional signature performs a three-dimensional role, as it is used to identify the signatory, express their will to be bound by the content of the instrument, and also as evidence of the physical presence of the parties to the act at the time of signing.

As for the electronic signature, it allows the identification of the signatory and the expression of their will to be bound by the content of the electronic instrument, but it also adds a new function represented in verifying the content of the electronic instrument and securing it against any changes that may occur.

The electronic signature is linked to the electronic document in a way that any subsequent modification requires a new signature. It also gives the electronic document the attribute of originality, as the electronically signed copy is considered the original copy, making it a document prepared in advance for evidence.

Section Three: Types of Electronic Signatures:

A- Classifications of Electronic Signatures:

With the advancement of modern technologies, several forms of electronic signatures have emerged, aiming to meet the conditions necessary for the legal recognition of the electronic signature. These forms include:

- Biometric signature.
- Electronic pen signature.
- Coded or secret signature.
- Digital signatures (which relies on encryption and are linked to private keys for decryption).

1- Biometric Signature

The biometric signature is performed using unique characteristics that distinguish each person²³, making it known as the "signature with intrinsic properties." This type of signature relies on the scientific fact that each individual has intrinsic qualities that differ from others and are relatively constant.

Biometric characteristics used in biometric signing include:

- Personal fingerprint.
- Retinal scan.
- Voiceprint.
- Lip print.
- Hand geometry.
- Personal signature.
- Strengths and weaknesses.

Although the biometric signature is characterized by high accuracy and security, it is not completely immune to forgery. A voiceprint can be recorded and replayed; using a special lip coating can make it similar to the original print; an eye print can be imitated using certain types of contact lenses.

Additionally, the vibrations carrying the sound or image can be copied and reused, leading to a loss of security and confidentiality.

Therefore, any means that performs the two functions of a signature, which are identifying its owner and confirming their will to be bound by the content of what is signed, is considered a valid signature.

2- Electronic Pen Signature:

Electronic pen signature is a modern method of biometric signing, where a person signs on a computer screen using a special electronic pen. This signature requires a computer with specific specifications to capture the signature accurately.

The signature image is stored in the computer's memory, and when a signed electronic document is sent, the sent signature is compared to the stored signature. Verification of the signature's validity depends on the pen movement and the shapes it takes, such as curves and twists, which are unique traits of the signatory.

Although forging this type of signature is considered more difficult compared to forging signatures on paper documents, thanks to the accuracy of the comparison process, it lacks the necessary security to rely on for evidence. The recipient can keep a copy of the signature and reuse it on any electronic document, enabling them to attribute it to the signature owner.

It is preferable to use this type of signature over Intranet or Extranet networks, as these networks are considered more secure than the Internet network, given that the transactors know each other.

3- Signature via Card Paired with Password (Coded Signature):

The secret signature often involves using plastic or magnetized cards equipped with electronic memory, used for signing electronic transactions. This method relies on a set of numbers or letters chosen by the signature owner, known only to them and those they inform, and is known by the abbreviation P.I.N.

The secret signature is commonly used in banking and electronic payment, where banks guarantee the organization of the proof process under an agreement with the cardholder. Cards include types such as:

Off-Line: Works with the American Express, MasterCard, and VISA systems.

On-Line: Requires special signing procedures.

The signing procedures are performed by inserting the card containing the client's data into the ATM machine, entering the client's secret password, known only to them, and issuing the withdrawal or payment order by agreeing to the operation by pressing the key that expresses the will to accept the operation.

French jurisprudence has recognized the electronic signature using cards paired with passwords and considered it fully valid for evidence, relying on the agreements concluded between the parties. However, this signature is not suitable for preparing written evidence ready for proof, because it is not attached to any written instrument, but is recorded in the bank's documents separately from any contractual document.

4- Digital Signature:

4.1-What Is a Digital Signature?

A *digital signature* is an electronic substitute for a manual signature that serves the same functions as a manual signature and more. It is an identifier created by a computer instead of a pen. Technically, a digital signature is the sequence of bits that is created by running an electronic communication through a one-way hash function and then encrypting the resulting message digest with the sender's private key. It is an unintelligible string of alphanumeric characters, such as the following:²⁴

As the foregoing makes clear, a digital signature is not anything like a handwritten signature. A digital signature is not a digitized image of a handwritten signature or a typed signature such as “/s/john doe.” Moreover, unlike a handwritten signature, which is unique to the signer, but presumably consistent across all documents signed, a digital signature is unique for each document signed. This is because a digital signature is derived from the document to be digitally signed. Any change to the document will produce a different digital signature.

A digital signature can serve the same purpose as a handwritten signature in that it may signify authorship, acknowledgment, or assent, among other things. However, digital signatures also serve important information security purposes that handwritten signatures cannot. A digital signature allows the recipient of digitally signed communication to determine whether the communication was created by the purported signer and whether it was changed since it was digitally signed. That is, a digital signature provides assurance as to the authenticity, non repudiability, and integrity of communication. Because a digital signature provides these security assurances, it is to this extent superior to a handwritten signature.²⁵

How Is Electronic Communication Digitally Signed?

Before a sender can digitally sign an electronic communication, the sender must first generate a public-private key pair. The private key (a large prime number) is kept confidential by the sender and is used for the purpose of creating digital signatures. The public key (another large, but related, prime number) can be disclosed generally by posting the key in online databases, repositories, or anywhere else the recipient of the digitally signed message can access it. To digitally sign an electronic communication, the sender runs a computer program that creates a unique message digest (or hash value) of the communication. The program then encrypts the resulting message digest using the sender's private key. The encrypted message digest is the digital signature. The sender then attaches the digital signature to the communication and sends both to the intended recipient.

A digitally signed communication looks like this:

October 30, 1998

Dear Order Department:

We commit to purchase 10,000 widgets at your price of \$175 per hundred.

Ship to:

Industrial Products Co.

555 Retail Drive

Chicago, Illinois 60061

Sincerely,

Purchasing Department,

Industrial Products Co.

——BEGIN SIGNATURE——

owHtWX1sU1UUP+91G+22ysbHhDHc BeZAVmq7L9iAuNJ2UuhX2soUSpaufVs
ftu8tby1kUXTGsGhAgsEY4h9b+EPBgA rBGNSELGpiNEFM5A80xIzEoPiPSEi
MRfbPfR/ajW7rIBjR/ZbfO/eed9+59917 7j3ndS9CWlcllqe3Dflw45vqJ85+dZ5hP
kywt6uOjb5zYvRmy2drFnZKT17a/97n/ Tt1ld8dNmyvqVl2K7jt8LxfVr9We2jHyk

——END SIGNATURE——

The digital signature process can be made very easy. With a user-friendly software interface, the user may complete the signature process by using a mouse to click on applicable buttons. No special technical expertise is needed to digitally sign a document. The end user should, however, appreciate the legal effects and consequences of digitally signing electronic communication.

Verifying a Digital Signature:

When a recipient gets a digitally signed communication, the recipient's computer runs a computer program containing the same cryptographic algorithm and hash function the sender used to create the digital signature. The program²⁶ automatically decrypts the digital signature (the encrypted message digest) using the sender's public key. If the program can decrypt the digital signature, the recipient knows that the communication came from the purported sender, that is, the

recipient has verified its authenticity. This is because only the sender's public key will decrypt a digital signature encrypted with the sender's private key.

The program then creates a second message digest of the communication and compares the decrypted message digest with the digest the recipient created. If the two message digests match, the recipient knows that the communication has not been altered or tampered with, that is, the recipient has verified its integrity. Prerequisites for Use of Digital Signatures The effectiveness of the digital signature process depends upon the reliable association of a public private key pair with an identified person. The discussion thus far has made one critical assumption. That is, that the public-private key pair of the sender does, in fact, belong to the sender.

Any assurance of authenticity/non repudiability would be worthless if the public key used to decrypt a digital signature belonged to an impostor and not the named sender. Paper signatures usually have an intrinsic association with a particular person because they consist of that person's unique handwriting. However, public-private key pairs used to create digital signatures have no intrinsic association with anyone because private and public keys are nothing more than large numbers. When a recipient obtains the public key of someone from whom he has received digitally signed communication, how does he know that the public key does, in fact, belong to the sender? An impostor could have generated the public private key pair and entered his public key in a public database under the recipient's name. The solution to this problem is to enlist a third party trusted by both the sender and recipient with performing the tasks necessary to associate a person or entity at one end of the transaction.²⁷

CERTIFICATION AUTHORITIES:

A certification authority (CA) is a trusted third person or entity that ascertains that a certain public key corresponds to a private key and that the public key belongs to an identified person. The certification process generally works in the following way. The user:

1. generates her own public/private key pair.
2. contacts the CA (either in person or online) and produces proof of identity, such as a driver's license and passport or any other proof required by the CA;
3. demonstrates that he or she holds the private key corresponding to the public key (without disclosing the private key). Once the certification authority has verified the association between an identified person and a public key, the certification authority then issues⁵⁸ a certificate.

A certificate is a computer-based record that attests to the connection of a public key to an identified person or entity. A certificate identifies the certification authority issuing it and the person (called a subscriber) identified with the public key. The certificate also contains the subscriber's public key and possibly other information, such as an expiration date for the public key. To provide assurance as to the authenticity and integrity of the certificate, the certification authority attaches its own digital signature to the certificate.²⁸

Conclusion:

Findings:

1- Regarding the Algerian Legal Framework: The Algerian legislator has demonstrated a genuine commitment to keeping pace with digital transformation by enacting Laws No. 15-04 (on electronic signatures) and No. 18-05 (on e-commerce). These texts constitute a coherent legal foundation granting electronic contracts legal validity and evidentiary value, aligning with international trends. However, the framework remains reactive rather than proactive, addressing

existing technologies without adequately anticipating future innovations. While the principle of functional equivalence between electronic and paper writing represents a significant legal achievement, its practical application faces challenges related to judicial awareness and technical infrastructure.

2-Regarding Electronic Signatures and Evidence: Digital signatures, relying on asymmetric encryption, provide the most secure and legally reliable form of electronic signatures, offering authenticity, integrity, and non-repudiation. Other forms such as biometric, electronic pen, and coded signatures offer varying degrees of security but fall short of digital signatures. The Algerian legislator's adoption of the UNCITRAL Model Law reflects appropriate international standards, yet the limited practical implementation of certification services hinders widespread adoption.

3- Regarding Comparative Legislation: Comparative study of Tunisian, Jordanian, Egyptian, and French legislations reveal consensus on regulating electronic contracts, with differences in drafting styles. French legislation stands out as the most developed, explicitly affirming the validity of electronically concluded contracts through Article 1127-1 of the Civil Code. The Algerian approach balances these models but would benefit from refinement, particularly regarding consumer protection provisions.

4- Regarding Consumer Protection and Digital Transformation: Electronic contracts place consumers in a vulnerable position due to the absence of face-to-face interaction and the cross-border nature of transactions. Algerian consumer protections remain insufficient compared to European standards. Additionally, the full potential of electronic contracts in supporting digital transformation remains unrealized due to limited digital infrastructure, low public awareness, insufficient judicial training, and the absence of a comprehensive national strategy.

Recommendations:

1-Legislative Development: The Algerian legislator should undertake a comprehensive review of the current framework, enacting a unified law addressing emerging technologies such as smart contracts and blockchain. The definition of the electronic contract should be expanded to include contracts concluded through automated systems and AI. Consumer protection should be strengthened by incorporating a clear right of withdrawal (at least 14 days), enhancing pre-contractual information requirements, and establishing accessible e-dispute resolution mechanisms.

2-Institutional and Administrative Measures: A specialized national authority for digital law should be established to monitor technological developments, license certification service providers, and propose legislative amendments. This authority should operate independently with adequate resources. A comprehensive national strategy for digital legal development should be created with clear objectives and performance indicators.

3-Judicial Training and Infrastructure: Specialized training programs for judges, lawyers, and court experts on electronic contracts and electronic evidence should be implemented. Investment in secure technical infrastructure is essential, including robust certification services and interoperable platforms. Public awareness campaigns should target both businesses and consumers regarding the legal validity of electronic contracts and electronic signatures.

4-International Cooperation and Research: Strengthening cooperation with UNCITRAL, the EU, and the Arab League is crucial to stay informed of international best practices. Bilateral agreements with trading partners should be pursued to establish harmonized rules for cross-border transactions. Academic research in digital law should be encouraged through research centers and integration into university curricula.

Citations:

¹ Ihuoma K. Ilobinso, (2016), Formation of Electronic Contracts, Commercial and Industrial Law Review, Vol. 2: 50, University of Lagos,P. 55.

² UNCITRAL – Model Law on Electronic Commerce (1996)

[https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce](https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce), accessed on: March 01, at 10:30 AM.

UNCITRAL – Model Law on Electronic Signatures (2001)

[https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures](https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures), accessed on: March 01, at 10:40 AM. See

Edwin Obimma Ezike, (2013), **Online Contracts In Nigeria – An overview**, Nigerian Juridical Review, vol 11, Faculty of Law, University of Nigeria, Enugu Campus, Enugu State, Nigeria, p.67.

Directive 2011/83/EU on Consumer Rights

<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0083>, accessed on: March 01, at 10:50 AM.

³ Essa al sulaiti law firm;electronic contracts, a study on the role of technological developmenis in the formation of the contract and the protection of the will of the contracting parties, May 2022, P 3, available at: https://www.eslaa.com/wp-content/uploads/2022/06/ESLF_Electronic-Contracts_May-2022_EN.pdf

, accessed on June 19, 2026, at 10.00 AM.

⁴ Matolla Adam, (2024), Electronic Contracts and their Legal Validity in Tanzania, International Journal for Multidisciplinary Research (IJFMR), Volume 6, Issue 6, India, p. 09.

⁵ Ibid, P.4

⁶ Tunisian Law No. 83 of 2000 concerning exchanges and electronic commerce.

<http://www.legislation.tn>, accessed on: March 02, at 09:30 AM.

⁷ Al Masadeh et al. –(January – June 2024) *The Electronic Contract in Civil and Commercial Codes* International Journal of Cyber Criminology Vol 18 Issue 1, p.4.

⁸ Egyptian Electronic Signature Law No. 15 of 2004, <https://www.cc.gov.eg>, accessed on: March 03, at 10:30 AM.

⁹ French Civil Code, article 1127-1. <https://www.legifrance.gouv.fr>, accessed on: March 03, at 11:50 AM.

¹⁰ Al Masadeh et al.op.cit.p.6.

¹¹ Ibid, p.7.

¹² Article 323 bis of Order No. 75/58, dated September 26, 1975, containing the Algerian Civil Code, amended and supplemented, Official Gazette No. 78 of 1975.

¹³ Article 323 bis 1 of the Algerian Civil Code.

¹⁴ Law No. 15/04 concerning electronic certification and signatures, dated 01/02/2015, Official Gazette No. 60 issued on 10/02/2015.

¹⁵ Mohamed Abdel Zaher Hussein, (2002) Legal Liability of Internet Networks, Dar Al-Nahda Al-Arabiya, Cairo, p. 8.

¹⁶ Mohamed Al-Saeed Rashdi, (2002)The Evidentiary Value of Modern Means of Communication, Dar Al-Nahda Al-Arabiya Library, Cairo, p. 3.

- ¹⁷ Omar Khaled Al-Zariqat, (n.d) The Contract of Sale via the Internet, PhD Thesis, Faculty of Law, Ain Shams University, Egypt, p. 2.
- ¹⁸ UNCITRAL –(2001) Model Law on Electronic Signatures, op.cit.
- ¹⁹ Mohamed Noor Jastanih, (2005) The Evidentiary Value of the Electronic Signature in E-Commerce Contracts, PhD Thesis, Faculty of Law, Cairo University, p. 165 et seq.; Abdel Aziz Al-Morsi Hammoud, (2002) The Evidentiary Value of the Electronic Instrument in Proof in Civil and Commercial Matters, Journal of Legal and Economic Research, Faculty of Law, Menoufia University, Egypt, Issue 21, p. 15 et seq.; Hatem Abdel Bari, (2004) The Evidentiary Value of Electronic Instruments, National Criminal Journal – National Center for Social Research, Vol. 47, No. 03, Egypt, p. 84 et seq.
- ²⁰ Ghazi Abu Arabi and Fayyad Al-Qudah, (2003) The Evidentiary Value of the Electronic Signature: A Study in Jordanian Legislation, Damascus University Journal for Legal and Economic Sciences, Vol. 20, No. 1, p. 169 et seq.
- ²¹ Law No. 15/04 concerning electronic certification and signatures, op.cit.
- ²² Article 7/5 of Law 15/04 concerning electronic signatures and certification.
- ²³ Fadila Yassad , (December 2024), The Role of Electronic Signatures in Consumer Protection: A Comparative Study, journal of human sciences, Algeria, Vol 35 N°3, P.107.
- ²⁴ Thomas J. Smedinghoff, ,(F all 1 9 9 8), E lectronic contracts and digital signatures, journal of equipment lease financing, vol. 1 6 / no. 2 (ELFA), USA , P.7.
- ²⁵ Ibid, P.8.
- ²⁶ Ibid,p.8.
- ²⁷ Ibid, P.9.
- ²⁸ Ibid,P. 9.

Bibliography:

Books:

- 1- Mohamed Abdel Zaher Hussein, (2002) Legal Liability of Internet Networks, Dar Al-Nahda Al-Arabiya, Cairo.
- 2- Mohamed Al-Saeed Rashdi, (2002) The Evidentiary Value of Modern Means of Communication, Dar Al-Nahda Al-Arabiya Library, Cairo.

Theses:

- 1- Omar Khaled Al-Zariqat, (n.d) The Contract of Sale via the Internet, PhD Thesis, Faculty of Law, Ain Shams University, Egypt.
- 2- Mohamed Noor Jastanih, (2005) The Evidentiary Value of the Electronic Signature in E-Commerce Contracts, PhD Thesis, Faculty of Law, Cairo University.

Scientific Articles:

- 1- Thomas J. Smedinghoff, ,(F A L L 1 9 9 8), E L E C T R O N I C C O N T R A C T S A N D D I G I T A L S I G N A T U R E S, journal of equipment lease financing, vol. 1 6 / no. 2 (ELFA), USA , P.7.
- 2- Abdel Aziz Al-Morsi Hammoud, (2002) The Evidentiary Value of the Electronic Instrument in Proof in Civil and Commercial Matters, Journal of Legal and Economic Research, Faculty of Law, Menoufia University, Egypt, Issue 21.
- 3- Ghazi Abu Arabi and Fayyad Al-Qudah, (2003) The Evidentiary Value of the Electronic Signature: A Study in Jordanian Legislation, Damascus University Journal for Legal and Economic Sciences, Vol. 20, No. 1.
- 4- Hatem Abdel Bari, (2004) The Evidentiary Value of Electronic Instruments, National Criminal Journal – National Center for Social Research, Vol. 47, No. 03, Egypt.
- 5- Edwin Obimma Ezike, (2013), Online Contracts In Nigeria – An overview, Nigerian Juridical Review, vol 11, Faculty of Law, University of Nigeria, Enugu Campus, Enugu State, Nigeria

- 6- Ihuoma K. Ilobinso, (2016), Formation of Electronic Contracts, Commercial and Industrial Law Review, Vol. 2: 50, University of Lagos.
- 7- Fadila Yassad , (December 2024), The Role of Electronic Signatures in Consumer Protection:A Comparative Study, journal of human sciences, Algeria,Vol 35 N°3
- 8- *Al Masadeh et al. –(January – June 2024) The Electronic Contract in Civil and Commercial Codes* International Journal of Cyber Criminology Vol 18 Issue 1.
- 9- Matolla Adam, (2024), Electronic Contracts and their Legal Validity in Tanzania, International Journal for Multidisciplinary Research (IJFMR), Volume 6, Issue 6, India.

Legal Texts:

- 1- Order No. 75/58, dated September 26, 1975, containing the Algerian Civil Code, amended and supplemented, Official Gazette No. 78 of 1975.
- 2- Law No. 15/04 concerning electronic certification and signatures, dated 01/02/2015, Official Gazette No. 60 issued on 10/02/2015.

Websites:

- 1- UNCITRAL – Model Law on Electronic Commerce (1996) [https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce](https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_commerce), accessed on: March 01, at 10:30 AM.
- 2- UNCITRAL – Model Law on Electronic Signatures (2001) [https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures](https://uncitral.un.org/en/texts/ecommerce/modellaw/electronic_signatures), accessed on: March 01, at 10:40 AM.
- 3- Directive 2011/83/EU on Consumer Rights <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011L0083>, accessed on: March 01, at 10:50 AM.
- 4- Tunisian Law No. 83 of 2000 concerning exchanges and electronic commerce, <http://www.legislation.tn>, accessed on: March 02, at 09:30 AM.
- 5- Jordanian Electronic Transactions Law No. 15 of 2015, <https://www.lob.gov.jo>, accessed on: March 02, at 10:30 AM.
- 6- Egyptian Electronic Signature Law No. 15 of 2004, <https://www.cc.gov.eg>, accessed on: March 03, at 10:30 AM.
- 7- French Civil Code, article 1127-1. <https://www.legifrance.gouv.fr>, accessed on: March 03, at 11:50 AM.
- 8- Essa al sulaiti law firm;electronic contracts, a study on the role of technological developmenis in the formation of the contract and the protection of the will of the contracting parties, May 2022, available at: https://www.eslaa.com/wp-content/uploads/2022/06/ESLF_Electronic-Contracts_May-2022_EN.pdf , accessed on June 19, 2026, at 10.00 AM.