



The Role of Electronic Signatures in Consumer Protection: A Comparative Study



Received: 25/05/2024 ;Accepted: 17/08/2024

*Fadila Yassad **

*Laboratory of Maritime Law and Maritime Ports in Algeria, University of August 20, 1955, Skikda (Algeria),
f.yassad@univ-skikda.dz*

Abstract

The tremendous development recently witnessed by humanity has led to a technological revolution that has transformed the world into a small village. With technological transformation, the forms and patterns of things have changed, casting its shadow on commercial activity and various business transactions. As a result, the concept of electronic signatures has emerged, which has become a means to extend legal protection to the electronic consumer.

Keywords

Electronic signature;
electronic consumer;
e-commerce;
electronic certification;
probative force.

الكلمات المفتاحية

التوقيع الإلكتروني؛
المستهلك الإلكتروني؛
التجارة الإلكترونية؛
التصديق الإلكتروني؛
القوة الثبوتية.

دور التوقيع الإلكتروني في حماية المستهلك: دراسة مقارنة ملخص

أدى التطور الهائل الذي شهدته البشرية في الآونة الأخيرة إلى ظهور ثورة تكنولوجية أصبح العالم بموجبها قرية صغيرة، وإثر التحول التكنولوجي تغيرت معه أشكال الأشياء وأنماطها، وهو ما ألقى بظلاله على النشاط التجاري ومختلف التعاملات التجارية، ونتيجة ذلك ظهرت فكرة التوقيع الإلكتروني الذي أصبح وسيلة من خلالها يمكن بسط الحماية القانونية للمستهلك الإلكتروني.

* Corresponding author. E-mail: f.yassad@univ-skikda.dz

Doi:

I- Introduction :

E-commerce and its accompanying developments have significantly impacted the legal system of traditional contracts, leading to the emergence of what is called cross-border online shopping, and the subsequent procedures for achieving electronic contracting, where the consumer is often one of the primary parties. From here, the need to protect the consumer in the electronic market began, as trust in the electronic market is paramount for consumers to meet their personal needs. Legal protection for the consumer, both during the electronic contract formation and its execution—this study will focus on the electronic contract formation stage and the preceding procedures—is very important because the consumer can be a weaker party. In such cases, the consumer may urgently need a particular good and thus may be subject to unusual and unfair terms imposed by the seller, who is the stronger party in this contract.

The basis of consumer protection in contracts in general, and electronic contracts in particular, lies in the consumer's vulnerability and the imbalance between them and the professional or expert providing the goods or services. This latter party is economically stronger and imposes its terms on the consumer. Moreover, in electronic contracting, the consumer does not see the goods physically in front of them nor touch them; they only view them through a computer screen.

In addition to the aforementioned, the consumer needs legal protection due to the risks, lack of security, and prevalence of problems across the electronic network. The protection of the consumer in electronic contracting is one of the most important and detailed subjects requiring research due to the novelty of this topic. Along with the development of electronic contracting, the world has become a large market within a small computer screen, through which one can access the desired site, review the purchase terms, contract, and access the specific goods or services. On the other hand, the emergence of large economic conglomerates in the electronic market has prompted many countries to hasten the enactment of legislations aimed at protecting the consumer in electronic contracting.

The problem of this study can be formulated in the following main question:

To what extent does the electronic signature play a role in providing legal protection to the consumer during the formation of the electronic contract?

To answer the study problem, we follow the following plan:

II. The Concept of Electronic Signature:

E-commerce saves consumers time and effort through open electronic markets, where the best quality product with the best price prevails (Mahbubi & Labboudi, 2005, p. 09). This allows commercial transactions to occur automatically and quickly. However, the Moroccan legislator has surrounded this trade with a series of guarantees to achieve trust and security. Therefore, the law on electronic exchange stipulates the necessity of having an electronic signature that meets specific conditions to confer a secure status as it is considered a legal proof in dealings with others. For further precaution and control in e-commerce, the legislator has also established a secure mechanism for creating the electronic signature to avoid any potential fraud or forgery that could affect the element of safety and trust assumed in commerce in general, and particularly in electronic commerce.

II.1. Electronic Signature Definition:

Several scholarly definitions of the electronic signature have been provided, one part of the scholarship defines it as: "An electronic signal or symbol logically connected to an electronic data message to identify the creator of the signature and confirm their identity and agreement to the information contained in the data message (Fawaz & Al-Matakah, 2008, p. 173)." Another perspective within the scholarship defines it as "a short unit of data carrying a mathematical mark along with the data contained in the document's content. (Al-Aibouki, 2009, p. 15)"

A third scholarly view defines it as: "Characters, numbers, symbols, or signals with a unique character that allow for the identification of the signature's owner and distinguish them from others, which is then recognized by the competent authority. (Mohamed, 2002, p. 171)"

These scholarly definitions define the electronic signature and illustrate its functional role in identifying the signature owner and distinguishing them from others.

As for the legislative definition of the electronic signature, it is defined by the UNCITRAL Model Law on Electronic Signatures in its Article 2 as: "Data in electronic form contained in, added to, or logically associated with a data message, which may be used to identify the signer in relation to the data message and to show the signer's consent to the information contained in the data message."

This definition emphasizes identifying the signer and indicating their consent to the information contained in the document, aligning with the general principle of a signature indicating the signer and affirming their intent to be bound by what has been signed.

Additionally, some laws do not distinguish between traditional and electronic signatures in terms of their functional roles. For instance, French Law No. 0 32/2000, dated March 13, 2000, states that a signature, in general, and an electronic signature, in particular, are necessary for the completion of a legal act. It serves to identify the person against whom it may be invoked and expresses the parties' agreement to the obligations arising from this act. When the signature is electronic, it requires a secure means to determine the person, ensuring their connection to the act they have signed, and the security of this means is assumed unless contrary evidence exists (Nassif, 2009, p. 238).

Arab legislations have shown interest in the electronic signature, with some of them enacting specific laws for it, such as the Syrian, Egyptian, and Algerian legislations.

The Egyptian legislator defined it as: "Something placed on an electronic document that takes the form of letters, numbers, symbols, signs, or others, having a unique character that allows identifying the signer and distinguishing them from others." This definition illustrates the connection of the electronic signature to the electronic document and provides examples of forms of electronic signatures (Nassif, 2009, p. 238), clarifying the functional role of the electronic signature in identifying the signer.

The Syrian legislator defined the electronic signature as: "A set of data inserted electronically on an electronic document, associated with it, and taking the form of letters, numbers, symbols, signs, or any other similar shape, having a unique character that allows identifying the signer and distinguishing them from others, and attributing a specific electronic document to them (Article 1; No. 4, 2009)." Then, it defined the electronic signature creation system as: "A means, electronic system, or software used to create the electronic signature," and the electronic signature creation data as "unique elements specific to the signer to distinguish them from others and used in creating the electronic signature."

The Syrian legislator, in defining the electronic signature, emphasized the electronic nature that the signature takes by using electronic data linked to the electronic document to express the identity of the signer and distinguish them from others.

The Algerian legislator also defined the electronic signature in Law 15-04 concerning electronic signing and certification, in Article 2, Paragraph 1, as "data in electronic form, attached or logically associated with other electronic data used as a means of authentication." The same article in Paragraph 3 specifically addresses the data related to creating the electronic signature, stating: "Unique data such as symbols and private encryption keys used by the signer to create the electronic signature." These definitions highlight the legislator's focus on the issue of authenticating the data subject to the signature rather than the signer's consent to the information in the document, emphasizing that the signer's intent is to be bound by what they have signed (Article 1; No. 15, 2004).

On the other hand, some Arab legislations have not enacted a specific law for the electronic signature but have regulated it through a unified law concerned with electronic commerce transactions, like the Bahraini legislation, which defines the electronic signature as: "Information in electronic form that exists in an electronic record and is affixed and logically associated with it, and can be used by the signer to prove their identity (Article 2; No. 2, 2002)."

The Electronic Commercial Transactions Law of Dubai defines an electronic signature as: "a signature composed of letters, numbers, symbols, sound, or a processing system in electronic form attached to or logically associated with an electronic message and stamped with the intention to authenticate or approve that message."

The Tunisian law has not recognized the electronic signature but merely defined the system for creating a signature as "a unique set of personal encryption elements or a set of equipment prepared to create an electronic signature." Consequently, it defined the system for verifying the signature as "a set of public encryption elements or a set of equipment that enables the verification of the electronic signature." It also defined encryption as "the use of codes or uncommon signals which render the desired information to be transmitted or sent unintelligible to others, or the use of codes and signals without which the information cannot be accessed⁽¹⁾." From these previous definitions, both doctrinal and legislative, it is evident that the electronic signature is a modern means to fulfill two conditions: identifying its owner and definitively confirming the owner's intent to be bound by the content signed. This arises through an electronic intermediary in response to the nature of transactions conducted electronically. Therefore, where contracts and deals are made electronically, the electronic signature is required, thereby excluding the concept of the traditional signature in its narrow sense.

II.2 Electronic Signature Characteristics:

It is noted that a handwritten signature is characterized by its uniqueness, permanence, and difficulty to forge—traits that are also found in the electronic signature, albeit with some differences. Although the electronic signature enables identification of the sender's identity, it does not guarantee the uniqueness of the signature as it inherently lacks the definitive ability to confirm that the signer is indeed the owner of the signature system. The signature system could potentially fall into the hands of others who might use it for their own purposes, yet the original owner remains liable for it, even if used by someone else. Thus, the legislator holds the owner of the encryption system fully responsible for any unauthorized use⁽²⁾. Moreover, the electronic signature is characterized by permanence, although the reality shows that this characteristic can change with the evolution of the technical means used, especially regarding the encryption system. As for the feature of being tamper-proof, it can be said that this is more readily achieved in the electronic signature than in the handwritten signature, especially when advanced encryption methods are employed (Kahloun, 2022, p. 285).

Nevertheless, the electronic signature possesses other characteristics that distinguish it from the handwritten signature, primarily in terms of speed and flexibility and confidentiality.

II.2.1. Speed and Flexibility:

The technology of electronic signatures has been utilized in the banking sector to complete transactions for withdrawals and electronic fund transfers using magnetic cards, which are divided into debit cards, payment cards, and credit cards. Regardless of their types, these magnetic cards are used after they are electronically read and the validity of the PIN, set by the customer, is confirmed. Subsequently, the completed banking transaction is recorded and all the data is electronically transferred to the central computer of the institution to automatically record the transaction in the customer's account.

The use of these cards has become so common in the banking sector that they have become the primary means of interaction between the bank and the customer. The ease of monitoring the PIN by the computer and the speed at which this monitoring occurs are the two features that have contributed to the widespread use of magnetic cards and led to the emergence of new and advanced technologies. One example of such technology is the integration of Minitel with a bank card equipped with memory, enabling individuals to meet some of their needs and purchase goods from their homes.

Moreover, the use of remote computing has provided a significant capability to conduct many electronic exchanges quickly and at minimal cost, which demonstrates the electronic signature's distinct advantages in terms of speed and flexibility.

II.2.2. Confidentiality of the Electronic Signature:

The confidentiality provided by the electronic signature is due to its reliance on a PIN that theoretically only the owner of the signature knows and is not easily disclosed. It typically consists of four numbers or letters and can be monitored by the computer automatically.

Over time, there has been a near consensus that in some banking transactions, the electronic signature may lead to disputes between the bank and its customer, such as when the bank deducts a certain amount from the customer's account based on an electronic withdrawal or a payment order. In response, the customer may dispute the existence or content of the claimed transaction and insist that no action on their part justifies the deduction from the deposited account balance.

II.3. Types of Electronic Signature:

The electronic signature generally consists of mathematical codes associated with an electronic document that represent the identity of its owner. These codes are referred to as "identification templates." The electronic signature has taken various forms, which continue to evolve with advancements in communication and information technology. Some of these forms are presented below.

II.3.1. Telex with Synchronous Encryption:

This can be defined as a technology primarily used in the banking sector among banks to identify each other through the use of telex in transmitting payment orders issued by their customers. The paying customer's bank drafts a telegram and sends it to the receiving customer's bank or to a foreign correspondent bank, requesting the payment of a specific monetary amount, mentioning the date of issuance and the name of the beneficiary. It then signs it by placing a known number, a key or code, at a corner of the telegram. This number is derived from a mathematical function that

considers all variables in the telex and is based on a secret rule known only to the sending and the receiving bank. Upon receiving the telex, the receiving bank decrypts the code to verify the authenticity of the correspondence by using the pre-agreed secret rule with the paying customer's bank. If the decrypted numbers match, it confirms that the telegram indeed comes from the issuing bank and complies with the payment order. If the numbers do not match, the receiving bank refrains from completing the transaction and immediately contacts the issuing bank to verify the command of that telegram.

II.3.2. The Secret Code:

The secret code is one of the applications of the electronic signature and is based on the smart card, which is a plastic card containing a smart chip. This chip is essentially a miniature computer no larger than the size of a fingernail. It can be programmed by entering certain information into its memory, such as the cardholder's name or institution, date of birth, and other data to fulfill specific functions. The smart chip programs an algebraic function or algorithm that generates the secret code for the customer, known as the "Personal Identification Number (PIN)." This number consists of four digits provided to the customer with the bank card based on a contract signed with the bank. By this contract, the customer agrees that inserting the card into the ATM and entering the PIN constitutes an electronic signature equivalent to their handwritten signature. As such, the customer cannot later deny any withdrawal transactions made using their bank card and PIN, even if they did not personally initiate those transactions, provided they have kept the PIN confidential and have not disclosed it to anyone by any means.

The use of the secret code technology has raised legal issues, with two contrasting positions in French judicial doctrine. The first position denies that the secret code qualifies as an electronic signature, while the second considers it an electronic signature capable of identifying its owner. The latter position was solidified in French jurisprudence following the landmark "Crédias" decision by the French Court of Cassation on November 8, 1989. This decision aligned with the stance of the Montpellier Court of Appeal, which recognized the legitimacy of the secret code as an electronic signature and based its rulings in favor of a financial institution whose customer disputed the existence of a banking transaction conducted using a payment card issued to him, relying on his secret code.

Consequently, there is a consensus in judicial doctrine that the secret code is an electronic signature, and thus, its formation inherently provides evidence of the cardholder's intent and willingness to commit to an action, whether it be an order, withdrawal, or fulfillment, depending on the nature of the bank card used.

II.3.3. Biometric Signature:

This type of signature relies on the physical characteristics of the person, including fingerprints, thumbprints, or iris patterns. It is the most commonly used method in applications. Practically, this method involves storing the image digitally and in a compressed format in the computer's hard memory or on a smart card. When the customer inserts their card into the reader of an ATM, the machine captures a real-time image of, for example, the iris, which is automatically logged into a digital record and compared with the digital record stored on the card or on the computer system. If there is a match between the two records, the identification is confirmed, and the transaction—whether a withdrawal or a payment—is processed. However, if a discrepancy between the records is found, the card is automatically retained by the machine because it is usually indicative of a stolen card. The likelihood of two individuals having the same iris pattern is approximately one in two hundred million (Caprioli, 1998, p. 587).

II.3.4. Dynamic Electronic Signature in Online Banking:

This signature allows the customer to conduct all their banking operations remotely via their personal computer. They issue commands using a small device, sealed and tamper-proof, no larger than a bank card. This device is an electronic calculator containing a smart chip ("Microprocessor") with a mathematical function that dynamically generates a secret code approximately every minute, synchronized with the online banking system. This makes the likelihood of hacking this code very low due to its constant variation. The signing process is completed as soon as the customer enters the number displayed on the computer screen. A distinctive feature of this device is that any attempt to tamper with its integrity results in its complete corruption and future inoperability.

II.3.5. Manual Electronic Signature:

This type of signature relies on a font set method, where each set contains 256 spaces designated for typographic characters, and the signature occupies one of these spaces. Anyone who wants to obtain a personal font set for their handwritten signature can send a sample of their signature to a specialized company via fax, along with a financial fee for the service. The company then prepares a personal font set for the handwritten signature, which can thereafter be installed on the computer and protected with a secret code for use when needed.

The manual electronic signature can also be created by scanning the handwritten signature using a scanner ("Scanarisation") and inserting it into a digital record, allowing it to be integrated into any application. However, the font set method is particularly economical in terms of hard memory usage because the signature only occupies one of the typographic character spaces in the set, whereas in the scanning method, the signature occupies a space equivalent to twenty-five thousand characters(Qartas, 2000, p. 114).

II.3.6. The Electronic Signature Based on Private and Public Keys:

Also known as the digital signature "La signature numérique," it differs from other forms of electronic signatures used in contexts where the parties know each other in advance and base their interactions on previously established contracts, either between banks or between banks and their customers, or on internal protocols governing interactions between departments and their agents. These conditions do not exist in the virtual, intangible world where the parties do not know each other and there are no pre-established contracts or protocols among them.

Therefore, the digital signature based on the private and public key system is considered the most suitable for the nature of transactions conducted over open communication networks, especially the internet. The private key is known only to the concerned party, while the public key is known to all participants. The public key is used to verify messages and electronic signatures created with the private key. The digital signature is used to authenticate electronic messages, but this signature differs from encryption technology in that the encoding "Codage" is limited only to the signature and does not extend to the content of the document exchanged electronically.

II.3.7. Automated Fulfillment:

This signature is achieved when a customer inserts their payment card, typically equipped with a magnetic strip, into an electronic reader and enters their personal PIN. Once the reader verifies the correctness of the PIN, it records the financial amounts related to purchases or services. These records are then sent directly from the electronic calculator at the point of sale to the central computer of the financial institution that issued the magnetic card. This computer then registers the financial amounts representing the purchases or services to the bank account of the provider, and correspondingly deducts those amounts from the account of the customer who benefits from the payment card.

Legally, the use of the payment card can be construed as a transfer order issued by the card beneficiary in favor of the creditor through the bank, whereby certain amounts are deducted from the account of the issuer and added to the account of the creditor.

III. Functions of the Electronic Signature:

While a handwritten signature is considered a means to create a visible and observable real-life situation, and a mere expression of an inner psychological state that translates acceptance into a tangible material form(Omar, 1997, p. 62), the electronic signature, in turn, serves as a means to validate legal transactions, even though it has an intangible and imperceptible character. Although applications of the electronic signature have resulted in various forms of electronic signatures, all these types perform two fundamental functions. The first is to identify the consumer, and the second is to verify the identity of the signer. Protection for this signature can be provided through:

III.1. Identifying the Consumer:

It has been mentioned that a handwritten signature ensures the definitive identification of the person performing the legal act based on three main pillars: the uniqueness of the signature, its inimitability, and its permanence—pillars that are not necessarily present in an electronic signature. In the digital world, a contractor cannot be certain that the electronic document sent to them is indeed from the person they assume they are dealing with over open communication networks. In such cases, the contracting does not occur between two individuals present in the same room but rather between individuals connected via a communication network. This situation is fraught with risks, including the possibility of one of the parties falling victim to fraud or deception, especially given that the creation of virtual storefronts on open communication networks has become a common occurrence in the digital world.

This phenomenon can be avoided, according to recommendations issued by the International Chamber of Commerce and some global conferences, by exercising caution and investigating the qualifications and status of the party before signing any electronic contract and by joining the Brussels Convention to benefit from its provisions related to compensation for fraud and deception incidents.

Nevertheless, the electronic signature can fulfill the function of identifying the owner of the digital correspondence since it relies on technical means and sophisticated mathematical equations that enable identification of

the signer. Generally, the electronic signature is based on the duality of the private and public keys, both of which are technically linked and neither is functional without the other.

However, the possibility that the signature system might be in the possession of another party and the potential for decryption remain concerns, albeit minimal, which can lead to erroneous identification processes. Therefore, some consider the biometric signature, which is linked to the physical attributes of the signer, as the most reliable form of electronic signature that ensures the uniqueness of the signature. Additionally, reliance on asymmetric cryptography, which is based on both public and private keys, is a technique that ensures the identification of the consumer.

Besides the function of identifying the owner of the document, the electronic signature can also ensure the process of verifying the identity of the signer.

III.2. Verifying the Identity of the Signer:

While the process of verifying the identity of the signer in the case of a handwritten signature can only occur subsequently, such as in the event of a dispute regarding the attribution of the signature to a certain individual or if the signed document is denied by the person to whom the signature is attributed, some legal experts have likened the roles and duties entrusted to a third-party verifier to those of a notary public or a public officer⁽³⁾ who is tasked with documenting transactions, preserving their originals, and issuing certificates related to the authenticity of electronic signatures and their attribution to their owners. Thus, the third-party verifier plays a pioneering role in monitoring the PIN of each party and ensuring the integrity and security of the information transmitted from sender to recipient without interfering in its content, and then providing all stakeholders with compelling evidence that substantiates the details of the electronic exchange of information. This evidence provides irrefutable proof, thereby demonstrating the effectiveness of the newly introduced electronic verification system, which ensures the security and safety of exchanges and e-commerce on open communication networks.

Although modern legislation focuses extensively on the functions of signatures, whether handwritten or electronic, primarily regarding identifying the contracting party and demonstrating their commitment to the content of the document, the Tunisian legislator has not focused on the functional aspect of the signature and has settled for the technical standard when defining it.

It might have been safer if the legislator had taken the opportunity during the revision to adopt the functional aspect of the signature in addition to the technical side in its definition, such as by emphasizing that the signature is only considered valid when it ensures identification of the document's owner and verifies the identity of the signer.

III.3.Means of Protecting Electronic Signatures in Algerian Legislation:

Through commercial transactions and the developments they have experienced, a range of methods has emerged that assist in protecting these transactions. However, there are advanced techniques by which the internet networks conducting these electronic commercial transactions are penetrated. To counter these issues and breaches, there has been a pressing need to devise ways to generally protect these transactions, and specifically the electronic signature from these attacks. This is manifested in technical protection as the first subsection and legal protection as the second subsection.

III.3.1. Technical Protection of the Electronic Signature:

To ensure the trust of users over the internet, it is essential to provide technical and artistic security against acts of electronic piracy. Given the increasing attacks on operations and exchanges conducted through electronic means and networks, in open networks, numerous legislations have intervened to establish a set of technical and artistic mechanisms to protect electronic transactions, particularly the focus of our study: the electronic signature. Among these mechanisms are encryption and electronic authentication.

A. Encryption Mechanism:

Encryption is a technical means that protects electronic commerce and the electronic exchange of data, thereby providing technical protection to the contracting parties and is integrally linked to the electronic signature. Encryption involves a set of technical messages aimed at protecting the confidentiality of data and information through special codes, commonly known as keys. The purpose of encrypting this data is to preserve its integrity and secure its privacy for the intended recipient. The encryption mechanism refers to any hardware or software, or both, that is created or modified to transform data—whether it be information, signals, or codes—based on confidential agreements, or to perform the reverse process, either under a confidential agreement or without it.

Providing encryption services involves every process aimed at using encryption methods for the benefit of others. The Egyptian Electronic Commerce Law defines it as "changing the form of data by converting it into codes or signals to protect these data from being accessed, modified, or altered by unauthorized parties."

Some jurisprudence defines it as "the process of disguising the message in a way that conceals the true content and renders it into unreadable codes," while other scholars describe it as "the science of secret writing and preventing unauthorized persons from decrypting this secret writing." Thus, from both legal and scholarly definitions, it is clear that to complete the encryption mechanism, two elements must be available: first, the presence of information and data intended to be encrypted, and second, the availability of a specific encryption mechanism to be applied to the data intended for transfer.

B. Electronic Authentication:

Electronic authentication is a secure method to verify the authenticity of a signature or document. Authentication authorities are among the most important technical means established by the legislator to protect the electronic signature. A neutral third party undertakes the task of verifying the electronic signature and its validity, performing the electronic authentication process. This individual acts as an intermediary between the parties to authenticate their electronic transactions. They issue electronic certificates that attest to the authenticity of the transactions included. These certificates establish a link between the signer and the signature creation data, thereby providing trust for intangible actions and exchanges.

III.3.2. The Probative Force of the Electronic Signature:

By recognizing the capability of electronic documents to perform the function of traditional physical documents and equating the two, and in the absence of regulatory texts and the establishment of structures and devices that embody this modern legislative direction, it becomes necessary to regulate the issue of electronic documents more precisely in terms of the limits and methods of applying the functional equivalence principle. We must discuss the legal validity of these documents under the existing statutes. Referring to the Civil Law, particularly Article 327 and subsequent sections, as well as Law 15-04, it can be said that the probative force of these documents establishes their validity among the parties involved, as well as to third parties, with the possibility of challenging them to diminish their value or exclude them entirely.

IV-Conclusion:

Through the study of the role of the electronic signature in consumer protection, we have reached a number of conclusions, which are as follows:

- The emergence of the idea of the electronic signature in various areas of life has been met with international, regional, and local efforts to regulate its legal framework and encourage its adoption. In fact, some of these legislations provide a specific and clear definition of the concept or nature of the electronic signature and have issued special legislation regarding it. This approach was followed by the Algerian legislator who amended the Civil Law in 2005 to recognize electronic forms of writing and adopted the electronic signature in Article 327, then issued Law 15-04 concerning the general rules for electronic signing and authentication. In these, the Algerian legislator adopted the principle of functional equivalence between electronic and traditional signatures.
- The electronic signature has the ability to fulfill the functions of a traditional signature, from identifying the signer to demonstrating the expression of will. Moreover, the electronic signature, in addition to these functions, surpasses the traditional signature in that it ensures the integrity of the document as it is considered a science, not merely an art. It is integral to the components of the electronic document itself and reveals any modifications or changes made to it.
- Electronic signature technologies come in various forms and are continuously evolving, with perhaps the best today being the digital signature that relies on a key. Each legislation has defined and regulated the issue of electronic signatures, focusing on the security of the technology and ensuring proper preservation of the document during its creation, transfer, and storage.
- For an electronic signature to gain evidentiary validity, specific conditions must be met to provide probative force. These conditions have been highlighted by various legislations, including the UNCITRAL Model Law, the European Directive on electronic signatures, and the Arab Model Law on Proof by Modern Means of Communication.

- The legal validity of an electronic signature as evidence depends on the level of security provided by the modern communication technology used by the contracting parties. Thus, many legislations strive to establish procedures that ensure security, trust, and legal protection for the electronic signature through its registration and authentication by a certified authority that issues authentication certificates and maintains custody of them. This authority operates under a license and is subject to the supervision and control of an administrative authority defined by each country's legislation, as done by the Algerian legislator.

Recommendations

- After presenting a summary of the findings from this study on our subject, we offer a set of recommendations or suggestions that we believe will help clarify and define the topic, especially in Algerian legislation:
- Enable notaries to have mechanisms that allow them to certify legal actions that require written documentation as a fundamental aspect of their establishment, thus allowing electronic technology to prevail in all forms and types of actions without legislation being an obstacle.
- The Algerian legislator should issue regulatory decrees related to the economic authority for electronic authentication, which would grant licensing to authentication service providers enabling them to issue electronic authentication certificates and thereby promote the use of qualified electronic signatures over simple electronic signatures.
- Expedite the installation of various devices for electronic authentication authorities, especially concerning the economic authority and the body responsible for accrediting the mechanisms for creating and verifying electronic signatures, due to its impact on the authentication of electronic signatures.
- Organize intensive training courses for judges and judicial assistants that cover the field of electronic evidence, particularly the technical aspects related to the creation of electronic documents and the operation of the electronic signature system, in line with the developments occurring in electronic commercial transactions.

Bibliography:

- [01] Al-Aibouki, A. R. (2009). Electronic Signature in Gulf Legislation, A Comparative Study. *Modern University Office*.
- [02] Article 1; No. 15. (2004). the Egyptian Electronic Signature Law.
- [03] Article 1; No. 4. (2009, 02 25). the Syrian Electronic Signature Law.
- [04] Article 2; No. 2 . (2002). the Dubai Electronic Transactions and Commerce Law.
- [05] Caprioli, E. A. (1998). Security and Trust in Electronic Commerce. *J.E Ped Générale*.
- [06] Fawaz, M., & Al-Matakah, M. (2008). *A Brief on E-Commerce Contracts* (01 ed.). Jordan: Dar Al-Thaqafa.
- [07] Kahloun, M. A. (2022). *Legal Aspects of Modern Communication Channels and Electronic Commerce*. Issahamats for Institutional Literature Publishing House.
- [08] Mahbubi, M., & Laboudi, H. (2005). E-Commerce, The Economic Environment of Business Projects. *Al-Ishaa Journal*(25).
- [09] Mohamed, A. Z. (2002). *Update on the Law of Evidence (The Status of Electronic Documents Among Written Evidence)*. Egypt.
- [10] Nassif, E. (2009). *The Electronic Contract, International Contracts in Comparative Law* (01 ed.). Al-Halabi Legal Publications.
- [11] Omar, M. B. (1997). The Evolution of Information Technology and Its Impact on Signatures. *Thesis for the Completion of Studies at the Higher Institute of Judiciary*.
- [12] Qartas, A.-M. (2000). The Validity of Electronic Signatures in Court. *Journal of Judiciary and Legislation*.

Note:

- [1]. Tunisian Electronic Exchanges and Commerce Law No. 83, 2000.
- [2]. Article 6 of Law No. 83 of 2000 related to Electronic Exchanges and Commerce states that "Anyone using an electronic signature system must take the minimum precautions to avoid any unlawful use of the encryption elements or personal equipment related to their signature." Article 7 adds that "If the user fails to fulfill these obligations, they are responsible

for any damages incurred by others as a result." Article 21 of the same law states that "The holder of the electronic certification is solely responsible for the confidentiality and integrity of the signature creation system they use, and any use of this system is considered to be from them."

- [3]. That analogy is somewhat exaggerated considering that the public official is assumed to be aware of the content of the documents since they would have drafted those documents or reviewed their content before certifying the signature on them. This does not apply to the third-party certifier, whose role is limited to ensuring the connection between the signature creation system and the verification system without reviewing the content of the electronic correspondence.