

Criminal Protection of Electronic Signatures in Algerian Legislation: An Analytical Study

Bouhali Naoual

Faculty of Law and Political Science, Lounici Ali University - Blida 2 (Algeria),

harounouh516@gmail.com

Received: 14/02/2026

Accepted: 08/04/2026

Published:22/04/2026

Abstract:

The gradual transition towards electronic signatures in various civil, commercial, and administrative transactions necessitates accompanying it with a modern legislative framework that provides the necessary legal protection, in order to preserve the interests of individuals from all forms of infringement. This prompted the Algerian legislator to enact Law No. 15-04, which defines the general rules relating to electronic signature and certification, alongside the relevant legal provisions of the Penal Code that include sanctions for criminal acts that affect electronic transactions in general and electronic signatures in particular.

Keywords: Electronic signature; digital signature; electronic transactions; criminal protection; penal code.

1. INTRODUCTION

The emergence of the phenomenon of most of the world's countries transitioning towards what is called e-government has been accompanied by a significant spread in the use of automated information systems and their reliance in almost all aspects of life. Practical reality has produced modern methods and means of dealing through the spread of electronic information processing systems that have begun to invade administrations, banks, and companies. Modern methods of dealing no longer align with the traditional concept of transactions, especially in the commercial field, and there is no place for manual procedures in their context. From here, everything manual has become an obstacle that is impossible to adapt with modern management and accounting systems, because contracting and completing many transactions necessarily require the presence of parties at the place of concluding the transaction so that they can sign the document proving this transaction. This led to the trend towards an alternative to that manual signature, which is the electronic signature, whose first beginnings appeared on the occasion of electronic payment operations at banks and financial institutions.

Given the paramount importance that the electronic signature enjoys in all legal transactions, whether civil, commercial, or administrative, it was incumbent upon states to surround it with a legal framework that clarifies its features and guarantees it legal protection that deters any act that might affect it, due to its serious reflection on electronic transactions and thus harm people's interests and violate their privacy. Like some countries of the world, the Algerian legislator sought to keep pace with this development occurring in the world of digitization, especially in the field of legal framework for electronic signatures. This raises a problem about the extent of the Algerian legislator's protection of the electronic signature and keeping it away from various forms of infringement?

To answer this problem, this study was divided into two sections: the first focuses on the concept of electronic signature, while the second focuses on the legal framework for criminal protection of electronic signatures, by following the descriptive analytical approach.

2. The Concept of Electronic Signature

Visions regarding the nature of electronic signatures have varied due to the multiplicity of angles from which this subject has been addressed, and there is overlap between the concept of electronic signature on the one hand and digital signature on the other hand, which requires distinguishing between the two concepts.

2.1 Definition of Electronic Signature

The subject of electronic signatures has attracted the attention of both jurists and legislators, resulting in different definitions between jurisprudence and law, which will be addressed in the following two branches.

2.1.1 Jurisprudential Definition of Electronic Signature

An electronic signature is a set of numbers that mix or blend with each other through complex mathematical operations to finally appear as a secret code specific to a particular person. Others have defined it as: "a short unit of data that bears a mathematical relationship with the data contained in the document's content"¹.

Some believe that an electronic signature is: "a person's expression of his will to commit to a specific legal act by creating secret codes known only to him." What is noticeable about this definition is that it is limited to that signature produced using encryption techniques (Cryptography or Encryption Techniques) - which is specifically termed digital signature - and did not take into account the various forms of electronic signatures, such as biometric signatures, whether represented by fingerprints, voice, lips, teeth, blood vessel pulses, or iris of the eye. The use of iris or voice print in electronic signatures does not constitute secret codes known to the owner of this signature, and therefore knowledge of secret codes is limited to some forms of electronic signatures and not others².

2.1.2 Legal Definition of Electronic Signature

The definition of electronic signatures in international legislation, comparative national legislation, and Algerian legislation will be addressed.

2.1.2.1 Legal Definition of Electronic Signature in International Legislation

This section will examine the most prominent international legislation represented by both UNCITRAL law and European Union directives.

2.1.2.1.1 Definition of Electronic Signature in UNCITRAL Model Law

Within the framework of efforts made by the United Nations represented by the United Nations Commission on International Trade Law to create a legal framework governing and regulating electronic commercial transactions, the UNCITRAL Model Law on Electronic Commerce was adopted, which is considered a reference for proving the validity and validity of electronic communication messages and acceptance and approval of electronic signatures on these documents and other authentication procedures used in commercial transactions³.

¹- Faisal Saeed Al-Gharib, *Electronic Signature and Its Authenticity in Evidence*, Publications of the Arab Administrative Development Organization, Egypt, 2005, p. 216.

²- Mohammed Amin Al-Roumy, *Legal System of Electronic Signature*, Legal Books House, Egypt, 2008, p. 14.

³- Omar Hassan Al-Moumani, *Electronic Signature and Electronic Commerce Law: A Comparative Legal and Analytical Study*, First Edition, Wael Publishing and Distribution House, Jordan, 2003, p. 75.

Referring to the text of Article Seven of the UNCITRAL Model Law on Electronic Commerce of 1996, we find that it referred to the electronic signature within a general framework clarifying its features; where this article stipulated that when the law requires a person's signature, this condition is considered fulfilled for a data message if a method is used that identifies that person and confirms his consent to the information contained in it, provided that this method is reliable in a manner commensurate with the purpose for which the message was created or sent, taking into account all relevant circumstances, including any related agreement. Unlike the UNCITRAL Model Law on Electronic Commerce, the UNCITRAL Model Law on Electronic Signatures of 2001 gave an explicit and direct definition of electronic signature, as Article Two of it stipulated that an electronic signature is electronic data that is inserted within a data message, added to it, or logically linked to it. It can be used to identify the signatory in relation to that message and to indicate his consent to the information contained in it. What is noticeable about the definition provided by this article is that it is inspired by the role played by the traditional signature as a tool for identifying the signatory and proving his consent to the document's content¹.

This definition of electronic signature is a comprehensive definition intended to encompass all forms and methods by which a document is signed electronically, whether currently available such as digital signature or those expected to be invented in the future. What is also noticeable about this definition is that this law follows the functional approach, where it focuses on the need for any signature to perform the main functions that the signature aims to perform, which are identifying the signature holder and expressing the signatory's consent to the content of the document he signs².

2.1.2.1.2 Definition of Electronic Signature in European Union Directives

The European Directive on Guidelines and Directives in the Joint Legislative Framework for Electronic Signatures issued on December 13, 1999, stipulated two types of electronic signature and set a specific definition for each type. In this regard, Article Two of the same law distinguished between Electronic signature and Advanced electronic signature, considering the first as information in electronic form related to and closely linked to other electronic information, used as an authentication tool, while the second is an electronic signature that must:

- Be uniquely linked to the signatory.
- Be capable of identifying and recognizing the signatory by using it.
- Be created using means in which the owner ensures complete confidentiality.
- Be linked to the information contained in the message so that it reveals any change in the information.

From the above, the European Directive stipulated two types of electronic signature: ordinary and advanced. The advanced signature is that signature that meets the four conditions mentioned above, noting that they are difficult conditions to achieve. The

¹- Mohammed Amin Al-Roumy, Op. Cit, p. 12.

²- Omar Hassan Al-Moumani, Op. Cit, p. 98.

ordinary electronic signature is that signature that resembles the UNCITRAL definition¹.

2.1.2.2 Legal Definition of Electronic Signature in Comparative National Legislation

National laws have followed the lead of the UNUCITRAL model law on electronic commerce in defining the electronic signature, especially since the content of this definition results in specific legal effects according to national legislation. Although it is not necessary for these national definitions to be uniform, they agree that the key factor is the presence of trust or reliability conditions in that signature in a way that provides it with full validity, just like the validity of a handwritten signature.

2.1.2.2.1 Definition of Electronic Signature in French Legislation

The French legislator gave a definition of electronic signature derived from the general definition of signature. Based on the text of paragraph four of Article 1316 of the French Civil Code, which was amended on March 13, 2000, the signature is generally defined as that signature necessary for the completion of a legal act and must identify the identity of its owner, and expresses the parties' consent to the obligations arising from it. When performed by a public official, it ensures the formality of the legal act. When the signature is in electronic form, it must be carried out using a reliable method to distinguish the identity of its owner and ensure its connection to the intended legal act. This definition given by the French legislator for electronic signature focuses on the necessity of performing the same traditional functions of signature, represented in distinguishing a person's identity and expressing his will to be bound by the legal act. However, it did not overlook the procedures for issuing and authenticating the electronic signature, which are generally handled by a person licensed by the competent authorities. These procedures ensure the personality of the signatory and his identification, and are carried out through means that enable the person to keep his signature under his control and do not allow others to steal it. They also ensure that the data signed by the person cannot be modified or tampered with².

2.1.2.2.2 Definition of Electronic Signature in Egyptian Legislation

The Egyptian legislator issued Law 15-2004 to regulate electronic signature, to keep pace with the development witnessed by economic life as a result of the transformation and orientation towards electronic commerce, as well as confronting those problems that emerged with the emergence of electronic transactions. Article One of the Egyptian law on electronic commerce defined electronic signature as: "letters, numbers, symbols, or signals that have a unique character that allows identification of the signature holder and his distinction from others"³.

¹ - Souad Kribat, Authenticity of Electronic Signature in Evidence, Master's thesis, Faculty of Law and Political Science, Blida 2 University, 2013-2014, p. 22.

² - Tharwat Abdel Hamid, Electronic Signature: Its Nature, Risks and How to Confront Them, The Extent of Its Authenticity in Evidence, New University House, Alexandria, 2007, p. 50.

³ - Faisal Saeed Al-Gharib, Op. Cit, p. 218.

What is noticeable about this definition provided by the aforementioned article is that it links the definition of electronic writing with the definition of electronic document. This means that, in the view of this law, an electronic signature is a mark, symbol, number, or letter written electronically on an electronic document, in a manner that identifies the attribution of that document to the signatory in a way that allows identification and distinction of the signatory's person and attribution of the electronic document to him.

However, this definition is criticized for expanding the scope of electronic signature, while some believe that it should be defined as: "the electronic imprint placed on the electronic document that indicates a logical connection between a specific person and the specific electronic document in a way that indicates that he is its creator, indicates his identity, and indicates his acceptance of its content." However, this does not mean that it prevents establishing an electronic statement indicating that the document bears the name of its creator in letters, symbols, or otherwise, meaning that the electronic signature is not necessarily the establishment of the name of the creator of the electronic document or a symbol for the lowest content, but the criterion is the availability of the logical evidence referred to, so this logic becomes a signature in the concept of that law¹.

2.1.2.3 Definition of Electronic Signature in Algerian Legislation

As a completion of his recognition of the authenticity of writing in its electronic form, the Algerian legislator recognized the electronic signature in Article 323 bis 2 of the Civil Code. The Algerian legislator also recognized the electronic signature through Executive Decree No. 07-162 dated May 30, 2007, relating to the operating system applied to each type of network, including wireless and electrical. However, what is noticeable about the above is that although the Algerian legislator actually recognized the electronic signature, he did not give it a definition clarifying its concept².

To remedy this matter, we find that the Algerian legislator became aware of this and attempted to provide a definition of electronic signature through Law No. 15-04³, where Article Two defined electronic signature as electronic data that is attached or linked to other electronic data, where this data is used as a means of authentication. The Algerian legislator also included in the same law another type of electronic signature called the qualified electronic signature, which Article Seven defined as that electronic signature that meets the following conditions:

- It is created based on a qualified electronic certification certificate.
- It is linked to the signatory and no one else.
- The signatory's identity can be determined through it.
- It is designed by a secure mechanism specific to creating the electronic signature.

¹ - Abdel Fattah Bayoumi Hegazy, *Electronic Signature in Comparative Legal Systems*, University Thought House, Alexandria, no publication date, p. 60.

² - Souad Kribat, *Op. Cit*, p. 25.

³ - Law No. 15-04 dated February 01, 2015, defining general rules related to electronic signature and certification, Official Gazette No. 6 issued February 10, 2015.

- It is created by means exclusively controlled by the signatory.
- It is linked to its special data that allows detection of any subsequent changes.

From our examination of the text of the two aforementioned articles, we conclude that the Algerian legislator distinguished in his definition of electronic signature between two types: the ordinary or simple electronic signature and the qualified or what is also called the secure electronic signature. Here we can also say that the Algerian legislator has thus adopted the same European approach regarding electronic signatures¹.

2.2 Distinction Between Electronic Signature and Digital Signature

Many have tended to confuse the use of the term Electronic Signature and the term Digital Signature. However, in reality, these two terms do not denote the same thing. Electronic signature is a broader and more comprehensive term referring to all possible means and methods for the signatory to produce his signature electronically for the purpose of authenticating the signed document or for the purpose of committing to the content of the signed document. It may include, for example, producing a person's signature by establishing an image of the handwritten signature issued by the signatory's hand and stored electronically on the document to be signed. It may also include producing a person's signature by typing the sender's name at the end of an email message or by using a secret number or code specific to the signatory's person (Personal Identification Number - PIN), as is the case in payment orders by credit cards and ATM credit cards. The signature can also be created using biological or physiological characteristics that are distinctive of the person and no one else, such as iris of the eye or fingerprint (Biometrics Technology, Biometric Signature)².

As for digital signature, according to international standards (ISO 7498-2), issued by the International Organization for Standardization and Measurement in 1988, it means a statement or information connected to another data system, or the formulation of a system in encrypted form, which allows the recipient to prove its source, verify the integrity of its content, and secure it against any modification or distortion³.

It should be noted that there are two types of encryption:

- Symmetric encryption: which is based on the idea of a secret number exchanged between the two parties and works in an isolated environment such as a plastic card, where the secret number is known to its owner and the device only.
- Asymmetric encryption: which relies on a pair of asymmetric keys: a public key known to everyone, and a private key whose knowledge is exclusively with its owner, who keeps it secret, through which he encrypts his message so that he cannot deny what is stated in it⁴.

¹ - Reference here to the European Directive law on guidelines and directives in the joint legislative framework for electronic signatures issued December 13, 1999.

² - Omar Hassan Al-Moumani, Op. Cit, p. 50.

³ - Tharwat Abdel Hamid, Op. Cit, p. 62.

⁴ - Souad Kribat, Op. Cit, p. 34.

For the electronic signature to be digitally completed, first, using algorithms, the written document is transformed from ordinary writing form into a mathematical equation, and the signature is transformed into numbers. For the document to be completed legally, it is necessary to place the signature on it, which is done by adding the numbers to the mathematical equation, where the document is completed and saved on the computer. No one can restore the document to its readable form except the person who has the equation for that, which plays the role of the key¹.

The digital signature system is used especially in banking transactions. An example of this is a credit card containing a secret number whose knowledge is restricted to the customer who inserts the card into the withdrawal machine when he wants to know his financial balance or withdraw part of it. Digital signature is also used in electronic correspondence between merchant suppliers and importers or between companies among themselves².

Whatever form it takes, the digital signature achieves the highest levels of trust and security for the document, ensures accurate identification and distinction of its parties, maintains the completeness of the legal work and its continuity in its original form, free from tampering and distortion, until the retention period ends. It also clearly expresses, without ambiguity or vagueness, the will of its owner to be bound by the legal act and accept its content. It thus has the conditions and guarantees required by the legislator in documents to be suitable as complete evidence in proof. In this context, it should be noted that despite the trust and security achieved by the digital signature, in a way that seems beyond fraud, piracy, and hacking operations, technically, thanks to scientific and technological progress, it is possible to carry out fraud and forgery operations by breaking the private key of the data message, whose equations are formulated in light of the public key. By obtaining the private key, it is easy to change the content of the data message, whether by its issuer or by the signature holder. With the acceleration of technological progress, specialized hackers can clone the private key by reformulating the equation starting from the public key at their disposal, then reformulating the data message according to their interests, then signing it with their own private key. Encryption technology specialists believe that the possibility of breaking the private key may occur within five to ten years, which is a real possibility that cannot be denied. They propose to address this by establishing an archiving system handled by a specialized body whose task is to certify the data message by placing its own signature on it through its own key, provided that this key cannot be hacked within a period of no less than twenty years³.

3. Legal Framework for Criminal Protection of Electronic Signatures

Like many international legislation, electronic signatures received a legal framework in Algerian legislation, the purpose of which is to establish special

¹ - Tharwat Abdel Hamid, Op. Cit, p. 62.

² - Abdel Fattah Bayoumi Hegazy, Op. Cit, p. 23.

³ - Tharwat Abdel Hamid, Op. Cit, p. 65.

protection criminalizing all forms of assault against it, whether in general laws (Penal Code) or in special laws (Law 15-04).

3.1 Protection Established for Electronic Signatures in the Penal Code

The Algerian Penal Code surrounded electronic signatures with criminal protection by criminalizing both the act of forging electronic signatures and the act of destroying electronic signatures.

3.1.1 Crime of Forging Electronic Signatures

Despite the agreement of world legislation on criminalizing the act of forgery in traditional documents, they were divided regarding the act of forgery occurring in the digital world in general and forgery of electronic signatures in particular. One side of jurisprudence sees the impossibility of applying traditional texts to computer forgery crimes, while another side sees the possibility of applying them.

Forgery of electronic signatures is achieved through counterfeiting or imitating an actually existing forgery or creating an electronic signature system and attributing it to a person other than its true owner. This crime is considered one of the intentional crimes, and the form of the moral element in it is the general criminal intent represented in the intention of forgery in the form of computer forgery. Accordingly, the perpetrator must know at the time of committing the forgery crime that this act is prohibited and punishable, and yet accept to do it, his will is directed to the act, and he accepts the consequences resulting from it. This is in addition to the availability of special intent in the crime of electronic signature forgery¹.

Referring to the general rules contained in the Penal Code, the Algerian legislator criminalized any behavior that constitutes an assault on the signature, whether by imitating it, creating an identical copy of it, or forging it partially or completely. To commit his criminal act, the perpetrator uses computer systems or computer programs designed for that purpose, such as software designed to break the code, access the numbers specific to the electronic signature, copy them, and then copy them again². The first paragraph of Article 214 of the Algerian Penal Code stipulates punishment for anyone who commits forgery in public or official documents by placing forged signatures while performing his function with life imprisonment, whether a judge or employee. Still within the framework of criminalizing forgery behavior, the first paragraph of Article 216 of the Algerian Penal Code included penalties for those who commit forgery in official or public documents by imitating or falsifying writing or signature. These penalties consist of temporary imprisonment from ten years to twenty years and a fine from 1,000,000 DZD to 2,000,000 DZD.

3.1.2 Crime of Destroying Electronic Signatures

¹ - Abdel Fattah Bayoumi Hegazy, Op. Cit, p. 542.

² - Boumediene Rahal and Noura Saadani, Criminal Protection of Electronic Signatures According to Algerian Law No. 15-04, Journal of Law and Political Science, Institute of Law and Political Science, Naama University Center, Volume 3, Issue 1, January 1, 2017, p. 239.

The act of destruction is achieved by depriving the computer program specific to the electronic signature of its ability to work. This is done in several ways, including spreading a computer virus or pouring a cup of water or liquid on the electronic medium on which it is stored. It should also be noted that using the same aforementioned methods leads to defecting the electronic signature in a way that deprives it of the ability to work or validity partially, such as issuing a distorted or unclear signature¹.

Like other computer crimes, the Algerian legislator addressed the crime of destroying electronic signatures. He stipulated this criminal behavior in Article 394 bis 1, which provides for punishment for anyone who fraudulently introduced data into an automated processing system, removed data from this system, or fraudulently modified it, with imprisonment from six months to three years and a financial fine from 500,000 DZD to 2,000,000 DZD.

According to the aforementioned article, the criminal act taken by the perpetrator in the crime of destroying electronic signatures targets the electronic signature for the purpose of changing the situation that the data or information of the electronic signature was in. According to the same article, the crime of destroying electronic signatures takes one of three forms: either introducing data into the automated processing system, removing the data it contains, or modifying it. For further clarification, what is meant by introducing data into the automated processing system is feeding the system with information to be processed or instructions necessary for the processing operation. In other words, it is adding new data to the medium designated for it, whether it was empty or had data on it before. Regarding the act of removing data contained in the automated processing system, it is removing part of the data recorded on a medium and present within the system, destroying that medium, or transferring and storing part of the data to the memory area. The act of modifying information means changing the data or information within the system and replacing it with other information².

Dr. Abdel Fattah Bayoumi Hegazy believes that destruction of electronic signatures cannot occur without extending to the electronic medium, which is a support on which electronic documents are recorded. It may be a CD or magnetic tape, or it may be the computer itself. This applies to Egyptian law, which defined the electronic medium as a tool, tools, or systems for creating electronic signatures³.

3.2 Protection Established for Electronic Signatures in Law No. 15-04 Defining General Rules Related to Electronic Signature and Certification

Like the Penal Code, Law No. 15-04 also surrounded electronic signatures with criminal protection by criminalizing both the act of disclosing the confidentiality of data and information and the act of collecting personal data of the signature holder without his consent.

¹ - Abdel Fattah Bayoumi Hegazy, Op. Cit, p. 542.

² - Aziza Lergat, Criminal Protection of Electronic Signature and Certification in Algerian Legislation, *Ijtihad Journal for Legal and Economic Studies*, Faculty of Law, Tamanrasset University Center, Volume 6, Issue 1, January 1, 2017, p. 115.

³ - Abdel Fattah Bayoumi Hegazy, Op. Cit, p. 543.

3.2.1 Crime of Disclosing Confidentiality of Data and Information

The greatest danger that most customers fear in electronic transactions through electronic contracting is lack of security. Therefore, most banks tend towards the encryption system through the customer's possession of an encrypted number known only to him in order to reduce electronic fraud. This requires recognition of the consumer's right to confidentiality of data and information and criminalization of assault on it. Therefore, any assault on data sent between the two parties to the contract through internet spaces constitutes an assault on the privacy and confidentiality of data and information sent between them, considering that such data enjoys privacy and confidentiality and expresses the will of the two parties to the contract to perform a legal act. Consequently, accessing this data or information can lead to harming the two parties to the relationship and violating their privacy by decryption¹.

The Algerian legislator emphasized maintaining the confidentiality of data and information. Article 42 of Law 15-04 stipulates the obligation to maintain the confidentiality of data by electronic certification service providers, as well as maintaining information related to the granted certification certificate. Penalties against those who assault the confidentiality of data and information were included in the same law. Article 70 stipulates punishment for electronic certification service providers who violate the provisions of the aforementioned Article 42, with imprisonment from three months to two years and/or a fine from 200,000 DZD to 1,000,000 DZD.

According to the aforementioned article, the crime of disclosing the confidentiality of data and information is achieved when the perpetrator discloses the confidentiality of information and data specific to the signatory's electronic signature, either by informing others of this information and data, or by allowing others to access the signatory's data without justification and legal basis, or by not securing electronic signature data as required by the fourth paragraph of Article 7 of Law 15-04, which confirmed the necessity that the electronic signature be designed by a secure mechanism specific to creating electronic signatures².

3.2.2 Crime of Collecting Personal Data of the Signature Holder Without His Consent

The basic role of electronic certification service providers is to enable the recipient to verify the identity of the sender and the validity of his signature. When one party places his electronic signature on an electronic document and sends it to another person, the electronic certification body issues an electronic certificate whose function is to link the signatory with his public key. This certificate contains data that identifies the signatory's identity to the recipient. The role of electronic certification service providers is limited to collecting personal data necessary for granting and maintaining the electronic certification certificate only. Exceptionally, the role of the same body in verification can extend to determining the legal capacity of the signatory, as well as

¹ - Tayeb Mouaffak Cherif, *Electronic Signature and Its Criminal Protection in Algerian Law*, African Journal of Legal and Political Studies, Ahmed Draia University of Adrar, Volume 01, Issue 01, June 20, 2017, p. 83.

²- Aziza Lergat, *Op. Cit*, p. 121.

verifying the matter of his authority to enter into contracting. This data cannot be used for other purposes¹. The Algerian legislator confirmed through Article 43 of Law 15-04 the necessity of electronic certification service providers' commitment to collecting personal data necessary for granting and maintaining the electronic certification certificate only, and with his explicit consent. By examining this article, it can be said that any violation of its provisions by electronic certification service providers constitutes one of two criminal behaviors:

First criminal behavior: Collecting personal data of the concerned person without explicit consent from the latter, where the perpetrator's criminal behavior here is represented by positive activity consisting of collecting data without the knowledge of its owner or collecting it despite the data owner's refusal to collect it. This case is also without the knowledge of the latter. The reason for the necessity of obtaining the concerned person's consent is that this data, although necessary for issuing the electronic certification certificate, affects the person's privacy itself and may extend to his family life.

Second criminal behavior: Using personal data for other purposes. The perpetrator's behavior in this case is positive behavior, which is using the personal data he collected based on his status as a certification service provider in other purposes not permitted, which are collecting it for granting and maintaining the electronic certification certificate. This act may also occur in the case of collecting data without the concerned person's consent, as in the first case².

To protect the signatory's personal data and deter those who assault it, the Algerian legislator included penalties against service providers when violating the provisions of the aforementioned Article 43. Article 71 of Law 15/04 stipulated punishment for electronic certification service providers who violate the provisions of the aforementioned Article 43 with imprisonment from six months to three years and/or a fine from 200,000 DZD to 1,000,000 DZD.

4- Conclusion

At the present time, electronic transactions have become an inevitable reality. The matter is not just slogans glorified by governments, but a necessary imperative to develop society and transition it to the digital world characterized by speed and high security. However, through our treatment of this subject, we concluded that this digital world can be penetrated, which makes people's data, including electronic signatures, vulnerable to danger. This prompted the Algerian legislator to surround this matter with attention and care through enacting laws that frame electronic transactions and provide them with legal coverage and protection, especially regarding electronic signatures, through the Penal Code and Law No. 15-04 as follows:

¹ - Radia Lalouch, Security of Electronic Signature, Master's thesis, Faculty of Law and Political Science, Mouloud Mammeri University of Tizi Ouzou, 2012, p. 113.

²- Boumediene Rahal and Noura Saadani, Op. Cit, p. 246.

- The Penal Code, which criminalized the act of forging electronic signatures, whose punishment may reach twenty years imprisonment and/or 2,000,000 DZD fine, and the act of destroying electronic signatures, whose punishment may reach three years imprisonment and/or 2,000,000 DZD fine.
- Law No. 15-04 defining general rules related to electronic signature and certification, which criminalized the act of disclosing confidentiality of data and information, whose punishment may reach two years imprisonment and/or 1,000,000 DZD fine, and the act of collecting personal data of the signature holder without his consent, whose punishment may reach three years imprisonment and/or 1,000,000 DZD fine.

No matter how much criminal protection the legislator provides for electronic signatures, it remains insufficient because technology develops at a very fast pace, and electronic transactions develop at the same pace. In parallel, crimes against these transactions proceed at the same pace as well. To curb this and provide more protection for electronic signatures, we suggest:

- Not relying on technical mechanisms to protect electronic signatures, and the necessity of accompanying them with legal mechanisms that raise the level of protection.
- The legislator's keeping pace with developments related to electronic signatures by amending general or special legal texts whenever necessary.
- The legislator's use of both technical and legal experts when drafting laws containing the legal framework for electronic transactions in general and electronic signatures in particular.
- Tightening penalties related to crimes against electronic signatures more in order to reach greater protection.

Bibliography List:

Books:

- Tharwat Abdel Hamid, *Electronic Signature: Its Nature, Risks and How to Confront Them, The Extent of Its Authenticity in Evidence*, New University House, Alexandria, 2007.
- Abdel Fattah Bayoumi Hegazy, *Electronic Signature in Comparative Legal Systems*, University Thought House, Alexandria, no publication date.
- Omar Hassan Al-Moumani, *Electronic Signature and Electronic Commerce Law: A Comparative Legal and Analytical Study*, First Edition, Wael Publishing and Distribution House, Jordan, 2003.
- Faisal Saeed Al-Gharib, *Electronic Signature and Its Authenticity in Evidence*, Publications of the Arab Administrative Development Organization, Egypt, 2005.
- Mohammed Amin Al-Roumy, *Legal System of Electronic Signature*, Legal Books House, Egypt, 2008.

Scientific Articles:

- Boumediene Rahal and Noura Saadani, Criminal Protection of Electronic Signatures According to Algerian Law No. 15-04, Journal of Law and Political Science, Institute of Law and Political Science, Naama University Center, Volume 3, Issue 1, January 1, 2017, pp. 234-262.
- Tayeb Mouaffak Cherif, Electronic Signature and Its Criminal Protection in Algerian Law, African Journal of Legal and Political Studies, Ahmed Draia University of Adrar, Volume 1, Issue 1, June 20, 2017, pp. 76-87.
- Aziza Lergat, Criminal Protection of Electronic Signature and Certification in Algerian Legislation, Ijtihad Journal for Legal and Economic Studies, Faculty of Law, Tamanrasset University Center, Volume 6, Issue 1, January 1, 2017, pp. 100-128.

Theses:

- Radia Lalouch, Security of Electronic Signature, Master's thesis, Faculty of Law and Political Science, Mouloud Mammeri University of Tizi Ouzou, 2012.
- Souad Kribat, Authenticity of Electronic Signature in Evidence, Master's thesis, Faculty of Law and Political Science, Blida 2 University, 2013-2014.

Legal Texts:

- Law No. 15-04 dated February 1, 2015, defining general rules related to electronic signature and certification, Official Gazette No. 6 issued February 10, 2015.
- Order No. 66-156 dated June 8, 1966, containing the Algerian Penal Code, as amended and supplemented.