Protection of Personal Data In accordance with Law No. 15-04, establishing the general rules relating to electronic signatures and certification.

Prof. Dr. Aggoni Mohamed
Faculty of Law and Political Science University of Biskra
Email: m.aggoni@univ-biskra.dz

Received: 14/09/2025 *Accepted: 26/11/2025* *Published:22/12/2025*

Abstract:

This study addresses the protection mechanisms established by the Algerian legislature in Law No. 15-04, which sets out the general rules relating to electronic signatures and certification,to protect the personal data and information of users.

The issue of protecting personal data in the virtual environment is considered an important topic, due to the technological progress that has led to the widespread spread of these transactions, and also due to the nature of the virtual environment in which the risks of violating the sanctity of private life are numerous, when undertaking the processes of collecting, storing, operating and processing personal data. This has prompted the Algerian legislator to work to create mechanisms capable of instilling trust and confidence among those using electronic media, to achieve the necessary protection of personal data from any electronic breach, manipulation, or fraud, this has been achieved by adopting encryption as a technical measure to protect electronic data and personal information, in addition to working to regulate the tasks of the electronic authentication authority and define its responsibilities.

Key words : data, electronic, character, Protection, personal.

Introduction :

Despite the advancement and prosperity brought by the digital revolution and technological development in this field, entering the virtual world is not free from new challenges that create several problems, the most important of which are security breaches and electronic piracy, which may lead to a lack of trust in the use of electronic data, especially personal data of customers, as a result of the lack of legal security in electronic transactions and the illegal exploitation of personal data during electronic processing.

Personal data constitutes an important part of the right to privacy, which the Algerian legislator has constitutionally guaranteed to protect, in accordance with the text of the fourth paragraph of Article 46 of the 2016 Constitution, which states the

following: “The protection of natural persons in the field of processing personal data is a fundamental right guaranteed by law, and its violation is punishable.”[1]

Personal data is considered any information of any type, regardless of its medium, as defined by the legislator in Law No. 18-07[2], relating to the protection of natural persons in the field of processing personal data, in the text of article 3 as follows: “It is any information, regardless of its support, relating to an identified or identifiable person, referred to below, “the person concerned”, directly or indirectly, in particular by reference to an identification number or one or more elements specific to his physical, physiological,genetic,biometric, psychological, economic,cultural or social identity.”

The issue of protecting personal data in the virtual environment is becoming increasingly important due to technological advancements and the widespread availability of these transactions, this is also due to the nature of the virtual environment, which is prone to data and personal data attacks, this makes it easy to manipulate electronic data and exploit it illegally and unethically for various purposes, whether by the data processors or third parties.

The Algerian legislator has worked to keep pace with the developments in the field of electronic transactions by issuing laws regulating transactions and accompanying them with texts to protect personal data ; he did not limit himself to placing penalties for attacks on personal data in the Penal Code, Law No. 18-07 also established preventive mechanisms to protect data in general and personal data in particular, which is what Law No. 15-04 included, which sets out the general rules related to electronic signatures and certification[3], which is the subject of our study.

The aforementioned law contains several provisions that provide the necessary protection for electronic documents and signatures that contain personal data, the importance and role of these two documents are clear to everyone, as they have become an alternative to traditional writing and traditional signatures, respectively, in proving actions and contracts based on electronic media and contributing to giving confidence to this type of transactions.

The spread of electronic contracts and transactions remains dependent on the availability of adequate technical and legal protection for the electronic transaction

[1] - Law No. 16-01 of March 6, 2016, amending the Constitution, Official Gazette No. 14 of March 7, 2016.
[2] - Law No. 18-07 of June 10, 2018, relating to the protection of natural persons in the pro-cessing of personal data, Official Gazette No. 34 of June 10, 2018.
[3] - Law No. 15-04 of February 1, 2015, establishing the general rules relating to electronic signatures and certification, Official Gazette No. 6 of February 10, 2015.

system, providing guarantees that encourage users to enter the virtual world with confidence that their information, personal data, transactions, and signatures are protected from fraud, leakage, or hacking.

Based on the above, we attempt to answer in our research an important question that represents the problem of the study, which we formulate as follows: What is the role and importance of the technical and legal mechanisms approved by the Algerian legislator in Law No. 15-04, which sets out the general rules related to electronic signature and certification, in achieving the required protection for personal data?

Based on this question, we will study the topic using an analytical and descriptive approach in two sections:
We will address encryption technology in the first section, and the role of electronic authentication authorities in protecting personal data in the second section.

First requirement : Encryption Technology.

Electronic writing and signature are contained within an editor on an electronic medium, hackers can penetrate personal information systems and take a picture of the editor and signature, or decode the latter, and then use it without the owner's knowledge, there are also numerous cases of credit card forgery, in addition to the emergence of viruses that threaten to damage saved files, which leads to disruption of dealing with electronic media;[1] failure to provide the necessary protection for personal data.

With reference to the text of Article 38 of Law No. 18/07, relating to the protection of natural persons in the field of processing personal data, which stipulates the following: "The person responsible for processing must put in place appropriate technical and organizational measures to protect personal data from accidental or unlawful destruction, accidental loss, damage, unauthorized publication or access.", we find that the legislator emphasized in the second paragraph of the same article that these measures must ensure an appropriate level of safety in view of the risks posed by processing and the nature of the data to be protected.

Based on the above, a mechanism has been put in place to protect personal data and electronic signatures in order to secure electronic transactions and e-commerce and overcome these difficulties, an encryption mechanism has been adopted to curb perpetrators of hacking, transgressions, and electronic fraud with the intent of harming electronic data, especially personal data.

[1] - There are many ways to fraud and infringe upon electronic data. See Nidal Ismail Barham, 2005, "Provisions of Electronic Commerce Contracts," Dar Al Thaqafa for Publishing and Distribution, First Edition, Amman, pp. 127-129.

Section One : What is meant by encryption?

The Algerian legislator did not address the definition of encryption in the E-Commerce Law, and was satisfied with defining the private encryption key and the public encryption key in Law No. 15-04, specifying the general rules related to electronic signature and certification, unlike the Egyptian legislator who defined it in the draft e-commerce law as a change in the form of data by converting it into symbols or signals to protect this data from being viewed, modified or changed by others.[1]
The Tunisian legislator defined in Article two of the Tunisian E-Commerce and Trade Law, it as ,the use of non-common symbols or signals that make the information to be written or sent incomprehensible to others, or the use of symbols or signals without which the information cannot be accessed.

Many definitions of encryption tools have been provided by jurisprudence, some have defined it as "the process of converting text into incomprehensible symbols and signals that appear meaningless to prevent others from viewing them except for persons authorized to view and understand the encrypted text, the encryption process focuses on converting general texts into encrypted texts with the possibility of returning the encrypted text to plain text after decryption with the encryption key that was created for encryption and decryption,[2] some scholars have adopted a technical definition, saying, "Encryption, coding, or coded writing is a technique based on an intelligent mathematical algorithm that allows someone who possesses a secret key to convert a readable message into an unreadable message and vice versa, that is to use the secret key to decode and return the encrypted message to its original state." [3]

The last definition makes it clear that encryption depends on mathematical operations by which the text to be sent is converted into symbols and signals whose content can only be understood by decoding and converting these symbols and signals into readable and understandable texts by using public and private encryption keys. Therefore, this process cannot be completed unless the recipient of the message has the encryption key that returns the signals and symbols to their original text.[4]

Based on the above, the encryption process consists of three interconnected elements:

[1] - Chapter One of the Egyptian E-Commerce Draft Law, Definitions.
[2] - Muhammad Fawaz Al-Matalqa, 2008, "A Brief Introduction to E-Commerce Contracts," Dar Al-Thaqafa for Publishing and Distribution, First Edition, Second Issue, Amman, p, 159.
[3] - Sultan Abdullah Mahmoud Al-Jawari, 2010, "E-commerce Contracts and the Applicable Law: A Comparative Study," Al-Halabi Legal Publications, First Edition, Beirut, p. 202.
[4] - Muhammad Fawaz Al-Matalqa, op. cit., p. 159.

1. The information to be encrypted.
2. The encryption algorithm that will be applied to the information, and the decryption algorithm that restores it to its original state.
3. Keys, which are one or more strings of codes based on complex mathematical formulas in the form of algorithms.[1]

The role of encryption is not limited to the functions of protection, security and confidentiality of personal information and contracts exchanged remotely on the Internet, but it also performs other functions related to verifying the identity of the person who signed, authenticating the content of the electronically signed document and ensuring its integrity, meaning ensuring that it has not been changed during transit within the communication network.[2]

Section Two : Encryption Controls.

The Algerian legislator has recognized the necessity of encrypting data and information. He also stipulated the need to work to preserve the confidentiality of encrypted data and information, in addition to considering the encrypted text to be electronically edited, we will discuss all of these controls in more detail below:

First: The legitimacy of data and information encryption: which is exchanged via electronic media, similar to what most comparative legislation has gone to in addressing legal texts dealing with data and information encryption, the Algerian legislator has approved, through Law No. 15-04, texts dealing with the encryption system, and defined private and public encryption, and authorized its use in electronic correspondence and commercial electronic transactions.

It emphasized the protection of encrypted data and the elements used in the encryption and decryption process from any attack, whether this was done by using personal encryption elements for signatures from non-parties of the relationship, or due to the use of encryption to commit fraudulent crimes, or the theft of encryption keys that decrypt the encrypted text and return it to the original text using the private encryption key.[3]

[1] - Belkacem Hamdi, 2015, "Concluding an Electronic Contract," a thesis submitted for a Doctor of Science in Legal Sciences, Business Law specialization, Faculty of Law and Political Science, University of Batna, p. 239.
[2] - Sultan Abdullah Mahmoud Al-Jawari, op. cit., p. 201.
[3] - Osama bin Ghanem Al-Obaidi, (no year of publication mentioned) "The Evidential Validity of Electronic Signatures," Arab Journal of Security Studies and Training, Volume 28, Issue 56, Kingdom of Saudi Arabia, pp. 158 and 159.

It is important to note that most Arab legislations in their texts on e-commerce dealt with the encryption process indirectly through electronic signatures, with the exception of Tunisian and Egyptian legislators, who dealt with the encryption process directly through special texts to avoid differences in interpretations and jurisprudential interpretations regarding it.[1]

Second : The right to maintain the confidentiality of encrypted data and information.

The Algerian legislator, through Law No. 15-04, considered that an attack on data sent between the two parties to the contract via electronic media is an attack on the privacy and confidentiality of data and information sent between the two parties to the relationship.

The legislator stipulates in Article 7,of Law No.18-07,that third parties may not access personal data subject to processing except in order to achieve the purposes directly related to the tasks of the person responsible for processing and the recipient, and the consent of the person concerned is not required if the processing is necessary to implement a contract to which the person concerned is a party or in order to implement pre-contractual measures taken at his request ; therefore, the confidentiality of the data used to create the electronic signature must be ensured by all available technical means at the time of approval, the provider of electronic certification services must also maintain the confidentiality of the data and information related to the electronic certification certificates granted, in accordance with the text of Articles 11 and 42 of Law 15-04.

Because this data and information is private and confidential and expresses the will of both parties to take a legal action, disclosing this data and correspondence to others could harm both parties to the contract and violate their privacy after decryption.

The Algerian legislature has enacted provisions that penalize anyone who violates the confidentiality of encrypted data or discloses it, whether by a third party, an electronic certification service provider, or the person in charge of auditing, This is in accordance with the provisions of the above-mentioned law, in the text of Article 68 and the following.

It remains to be noted, with regard to encryption technology, the necessity of keeping pace with the rapid development of technology. What seems impossible today in terms of the possibility of hacking encryption may be permissible in a few years,

[1] - Muhammad Fawaz Al-Matalqa, op. cit., p. 161.

furthermore, the encryption system may contain loopholes in its design that could be exploited to reveal the encrypted message.

Third : Considering the encrypted text as an electronic document.

As a result of the legislator's recognition of the encrypted text and its validity in proving all legal transactions that take place via electronic media, it is considered an electronic document even though it is not understood by the public, thus, the signs and symbols are converted into readable and understandable texts that serve as evidence against anyone who violates the commitments made by both parties to the agreement.[1]

Section Three : Encryption Methods.

Cryptographic techniques in computer science can be classified into two main categories based on the type of key used in encryption.

First:The private key (symmetric encryption technology) : It is a system of encrypted writing with a private key, it works by using a single key, known as a private key, that is owned by both the sender and receiver of the message, therefore, this type of encryption technology uses the same key or secret code to encrypt and decrypt messages. The two parties to the relationship initially agree on a password to be used in the encryption and decryption that has been prepared, when a password is entered, the passphrase is converted into a binary number that computers can understand, when the message is sent to the other party, in order for them to be able to read it, the ambiguity must be removed and the message must be shown in its original form by using the password with which the encryption process was carried out.[2]

This technology is criticized for using the same key by two different people (sender and recipient), which may weaken the authenticity and probative force of digital documents and electronic signatures, based on the constant risk that the private key may have been leaked or transferred illegally, given the difficulty of determining the source of the leak or transfer, in addition, using this technology forces the recipient of encrypted messages coming from different sources to acquire a number of private keys equal to the number of messages coming from these sources, which is considered a cumbersome matter.[3]

Second : Public key (asymmetric encryption) : Unlike private key encryption, the same key is not used to encrypt messages. Instead, two different secret keys are used to decrypt them. The first is private and owned by a specific user of electronic media, who

[1] - Osama bin Ghanem Al-Obaidi, op. cit., p. 160.
[2] - Muhammad Fawaz Al-Matalqa, op. cit., pp. 163 and 164.
[3] - Sultan Abdullah Mahmoud Al-Jawari, op. cit., pp. 203 and 204.

keeps it secret and private to him, while the second is public and is distributed to other users from whom he wants to receive encrypted messages.[1]

Thus, two different keys, linked mathematically, are used to create the electronic signature for transferring data and information, then it is installed again using the asymmetric encryption system, if others know the public encryption key, they cannot discover the signer's private key and use it to identify the content of the message, the private key is known to only one party, it is the sender's key and is used to encrypt or decrypt the message, while the public key is usually known to more than one party or person.[2]

This technology has achieved significant practical and legal advantages, allowing each user in electronic transactions to use a single key or secret code to encrypt the messages they wish to send, or to decrypt the message they receive. Although there are difficulties facing this type of encryption, primarily related to ensuring the public key, that is, it actually belongs to the user who holds the private key, but this obstacle was resolved through the intervention of a neutral and independent third party, the electronic certification authority.[3]

Second requirement : The role of electronic authentication bodies in protecting personal data :

Public key encryption technology requires the intervention of a neutral and independent third party between the holder of the private key and the holder of the public key. This person is called the third party authenticator, who provides authentication services.

The establishment of the electronic authentication authority was not only for the purpose of facilitating and monitoring electronic transactions, but it is also considered one of its priorities to ensure legal security and protect electronic transactions, especially electronic signatures and personal data, from the dangers that may face them due to the nature of these transactions, which are conducted via electronic media and between people and dealers who are brought together by a virtual contract council, which is what the legislator stipulated in Article 43 of Law 18-07, as follows : If the processing of personal data in electronic communications networks open to the public results in its destruction, loss, disclosure or unauthorized access, the service provider must immediately inform the national authority and the person concerned, if this results

[1] - Muhammad Fawaz Al-Matalqa, op. cit., p. 165.
[2] - Osama bin Ghanem Al-Obaidi, op. cit., pp. 160 and 161.
[3] - Fadi Muhammad Imad al-Din Tawkal, 2010, "Electronic Commerce Contract," Al-Halabi Legal Publications, First Edition, Beirut, p. 155.

in an infringement on his personal life, unless the national authority considers that the necessary safeguards for the protection of the data have been taken by the service provider.

One of the most important legal guarantees for protecting and preserving the integrity of documents containing personal data and electronic signatures is the issuance of an electronic authentication certificate proving this, verifying the identity of the signatory, as well as proving the content of the electronic data and issuing encryption keys.

Section One : Issuing an Electronic Certification Certificate.

The Algerian legislator distinguished between a simple electronic certificate and the electronic certificate described in Article 3 bis of Executive Decree No. 07/162,[1] the former was defined as: "A document in electronic form that proves the connection between the data of the electronic signature examination and the signatory.". The latter is: "An electronic certificate that meets the specified requirements." ; The Algerian legislator then returned to this point in Law No. 15-04, to clarify in more detail the difference between the two certificates, he kept almost the same definition of the authentication certificate in the text of Article 2/7, while he elaborated on the definition of the described electronic authentication certificate in Article 15 of Law 15-04, saying:"the described electronic authentication certificate is an electronic authentication certificate that meets the following requirements:

1- It must be granted by a trusted third party or by an electronic certification service provider in accordance with the approved electronic certification policy.

2- It must be granted exclusively to the signatory.

3- It must include, in particular:

A. An indication that this certificate was granted as a described electronic certification certificate.

B. Identification of the trusted third party or authorized electronic certification service provider issuing the electronic certification certificate, as well as the country in which they reside.

C. The signatory's name or pseudonym that allows their identification.

D- The possibility of including a special attribute for the signatory, if necessary, depending on the purpose of using the electronic certification certificate.

E- Data related to the verification of the electronic signature,consistent with the data for creating the electronic signature.

F- Indicating the start and end dates of the electronic certification certificate's validity.

G- The identification code of the electronic certification certificate.

[1] - Executive Decree No. 07-162, dated May 30, 2007, amending and supplementing Executive Decree No. 01-123, dated May 9, 2001, relating to the operating system applicable to all types of networks, including wireless electrical networks, and to various wired and wireless telecommunications services.

H- The electronic signature described for the electronic certification service provider or the trusted third party granting the electronic certification certificate.
I- Limits on the use of the electronic certification certificate, if applicable.
J- Limits on the value of transactions for which the electronic certification certificate may be used, if applicable.
K- Reference to the document proving the representation of another natural or legal person, if applicable.

Upon examining the above-mentioned texts, it becomes clear to us that a simple electronic certificate requires procedures related to data and information related to verifying the signature of a specific person and confirming the identity of that person. As for the described electronic authentication certificate, it is related to issuing a type certificate according to conditions set by the legislator, including that it includes, in particular, the described electronic signature.

It is clear from the above that both certificates fulfill the requirement that an electronic signature be linked to an electronic certificate issued exclusively by an accredited electronic certification authority. Therefore, an electronic certification certificate must be available for the electronic signature to be described.

The legislator stipulated in Law No. 18-07,mentioned above, According to the text of Article 42, that personal data collected by the provider of electronic certification services for the purposes of delivering and storing certificates related to electronic signatures must be obtained from the persons directly concerned, except in the case of their explicit consent, it may not be processed for purposes other than those for which it was collected.

The information contained in the certificate is verified using the public key of the person who issued the certificate, this certificate includes the public key in addition to the rest of the details that show that the signatory specified in the certificate has the private key corresponding to the public key contained in the certificate, this allows the recipient of the certificate to use the public key mentioned in it to verify that the electronic signature was created from the corresponding private key, and that the message has not been changed since it was signed.[1]

[1] - Alaa Ahmed Mohammed Haj Ali, 2013, "Legal Regulation of Electronic Signature Certification Bodies," a thesis in fulfillment of the requirements for a Master's degree in Private Law, Faculty of Graduate Studies, An-Najah National University, Nablus, Palestine, p. 57.

Section Two : Verifying the Identity of the Signatory.

The Algerian legislator stipulates in Article 44 of Law No. 15-04; that the provider of electronic certification services must verify the integrity of the creation data with the signature verification data before granting an electronic certification certificate, The provider of electronic certification services shall grant one or more certificates to each person who submits a request, after verifying his identity and, where necessary, verifying his special characteristics, in the case of legal persons, the provider of electronic certification services shall keep a record in which he records the identity and characteristics of the legal representative of the legal person using the signature related to the electronic certification certificate described, so that the identity of the natural person can be determined upon each use of this electronic signature.

By issuing an electronic certification certificate, the certification authority, certification service provider, or certification service provider ensures that third parties have confidence in the validity of the data it contains, particularly with regard to the identity of the signatory and the attribution of the electronic signature to him, this encourages those who read it to enter into contracts with confidence and reassurance.[1]

The certification authority is also responsible for providing those relying on this electronic certificate with the means to prove that the person identified in the certificate was in control of the signature device and that it was valid at the time of the signature.[2] Furthermore, Article 43 of Law No. 18-07 states ,requires every service provider to maintain an up-to-date inventory of violations related to personal data and the measures taken in this regard.

Section Three : Proof of the Content of Electronic Exchange.

The Algerian legislator stipulated in Article 45 of Law No. 15-04, that the provider of electronic certification services shall revoke the electronic certification certificate described if it is proven to have been granted based on false or forged information, if the information contained in the electronic certification certificate no longer corresponds to reality,or if the confidentiality of the signature creation data has been breached.

The responsibilities of the authentication authority include verifying the content of electronic exchanges between parties, ensuring their integrity and freedom from fraud or deception, as well as proving their existence and content, the authentication authority

[1] - Hala Al-Hassan, 2010, "Electronic Signature Authentication," Damascus University Journal of Economic and Legal Sciences, Volume 26, Issue 1, p. 531.

[2] - Zahra Kisi, June 2012, "The Legal System for Electronic Authentication (Certification) Authorities," Policy and Law Notebook, Issue 7, p. 216.

monitors commercial websites and ensures their actual existence and credibility,[1] if it becomes clear that these websites are not serious or genuine, it warns users.

Therefore, the aim of the certification body is to ensure the safety and security of transactions via electronic media, in terms of its parties, content, location and date.[2]

Section Four : Issuing Electronic Keys.

Among the duties of the electronic authentication authority is issuing the private key used to encrypt the electronic transaction and the public key used to decrypt it.[3]

It authenticates the identity of the person holding the public key and issues electronic certificates that guarantee that the public key belongs to the party holding the private key. The public key is then used to decrypt the original message and ensure that it has not been modified.[4]

Conclusion :

Through this research, I have sought to shed light on the technical and legal means approved by the legislator in Law No. 15-04, which support the protection of personal data and information from electronic piracy and breaches, and prevent third parties from accessing, intercepting, modifying, or distorting data messages exchanged over the Internet Or modifying, distorting, fraudulently using electronic forgery or using a third party's signature without their knowledge, in order to maintain its confidentiality and privacy for the parties, using digital electronic means or specific codes.

The continuity of e-commerce and its ongoing use necessitates the implementation of preventative measures to protect the personal data of users, editors, and electronic signatures, which require a secure global information infrastructure to provide users with confidence and security, in order to address most of the risks facing users of electronic media.

[1] - Khaloui (Anan) Nasira, 2013, "Legal Protection of Consumers via the Internet - A Comparative Study," Master's Thesis in Law, Mouloud Mammeri University of Tizi Ouzou, Faculty of Law and Political Science, p. 164.

[2] - Samir Saad Rashad Sultan, (Not Mentioning the Number and the Year of the Evil), "Electronic Authentication: A Comparative Study," Journal of the Faculty of Law, Mansoura University, p. 6.

[3] - Lazhar Ben Saeed, 2012, "The Legal System of E-Commerce Contracts," Dar Houma for Printing, Publishing, and Distribution, Algeria, p. 177.

[4] - Mahmoud Abdel Rahim Al-Sharifat, 2011, "Consensus in Forming a Contract via the Internet," Dar Al-Thaqafa for Publishing and Distribution, second edition, Amman, p. 204.

We have reached several results when presenting this study, the most important of which is that the Algerian legislator, after the issuance of Law No. 15-04, tried to keep pace with the development in protecting electronic transactions and personal data and adding legal security to users of electronic documents and signatures by stipulating the process of electronic encryption as a technical means that relies on encryption keys, protecting electronic data from external hacking that threatens the integrity of transactions. Encryption provides the highest degree of security and protection for Internet users, thanks to the use of the best encryption methods that are difficult to crack. Although the legislature has not detailed the encryption mechanism, it has approved the implementation of this system, which is considered the technical guarantee used globally.

The legislator also stipulated, in addition to the use of encryption technology, a system of authenticated certificates implemented by a third party to confirm that the real client is the one dealing with the signatory by issuing electronic certificates showing the attribution of the electronic signature to its owner and verifying the identity of the signatory and the connection of the signature to the electronic document and its integrity, in addition to verifying the integrity of the electronic data and issuing the electronic keys used in the encryption process, by combining these two methods-encryption and authentication-we ensure the confidentiality of personal data and business transactions, as well as the protection of documents and electronic signatures for secure transactions.

Finally, we highlight the most important recommendations we have reached below :

1- It would be preferable if the legislator stipulated the encryption mechanism, its types, and methods of working with it in order to give legal status to this important technology in ensuring the safety of personal data and electronic transactions.

2- Educating customers about the importance of taking caution and care in their electronic transactions and the necessity of using the described electronic signature, which is characterized by greater protection than a simple electronic signature.

3- The necessity of training judges in the field of electronic disputes, and organizing special seminars and training days related to the protection of electronic data and personal data of users in the electronic environment.

Bibliography List

1/The Sources:

1- Executive Decree No. 07-162, dated May 30, 2007, amending and supplementing Executive Decree No. 01-123, dated May 9, 2001, relating to the operating system applicable to all types of networks, including wireless electrical networks, and to various wired and wireless telecommunications services.

2- Law No. 15-04 of February 1, 2015, establishing the general rules relating to electronic signatures and certification, Official Gazette No. 6 of February 10, 2015.

3-Law No. 16-01 of March 6, 2016, amending the Constitution, Official Gazette No. 14 of March 7, 2016.

4- Law No. 18-07 of June 10, 2018, relating to the protection of natural persons in the pro-cessing of personal data, Official Gazette No. 34 of June 10, 2018.

2/ the References:

First:books

1- Fadi Muhammad Imad al-Din Tawkal, 2010, "Electronic Commerce Contract," Al-Halabi Legal Publications, First Edition, Beirut.

2- Lazhar Ben Saeed, 2012, "The Legal System of E-Commerce Contracts," Dar Houma for Printing, Publishing, and Distribution, Algeria.

3-Muhammad Fawaz Al-Matalqa, 2008, "A Brief Introduction to E-Commerce Contracts," Dar Al-Thaqafa for Publishing and Distribution, First Edition, Second Issue, Amman.

4- Mahmoud Abdel Rahim Al-Sharifat, 2011, "Consensus in Forming a Contract via the Internet," Dar Al-Thaqafa for Publishing and Distribution, second edition, Amman.

5-Sultan Abdullah Mahmoud Al-Jawari, 2010, "E-commerce Contracts and the Applicable Law: A Comparative Study," Al-Halabi Legal Publications, First Edition, Beirut.

Second: Theses and Dissertations

1-Belkacem Hamdi, 2015, "Concluding an Electronic Contract," a thesis submitted for a Doctor of Science in Legal Sciences, Business Law specialization, Faculty of Law and Political Science, University of Batna.

2- Alaa Ahmed Mohammed Haj Ali, 2013, "Legal Regulation of Electronic Signature Certification Bodies," a thesis in fulfillment of the requirements for a Master's degree in Private Law, Faculty of Graduate Studies, An-Najah National University, Nablus, Palestine.

3- Khaloui (Anan) Nasira, 2013, "Legal Protection of Consumers via the Internet - A Comparative Study," Master's Thesis in Law, Mouloud Mammeri University of Tizi Ouzou, Faculty of Law and Political Science.

Third: Journal article

1- Hala Al-Hassan, 2010, "Electronic Signature Authentication," Damascus University Journal of Economic and Legal Sciences, Volume 26, Issue 1.

2- Osama bin Ghanem Al-Obaidi, (no year of publication mentioned) "The Evidential Validity of Electronic Signatures," Arab Journal of Security Studies and Training, Volume 28, Issue 56, Kingdom of Saudi Arabia.

3- Zahra Kisi, June 2012, "The Legal System for Electronic Authentication (Certification) Authorities," Policy and Law Notebook, Issue 7.