THE NATURE OF THE BUYER'S ELECTRONIC FULFILLMENT RISKS- REALITY AND CHALLENGE

[1]KORICHIRAZIKA ,[2] LEMOUCHIA SAMIA
korichi-razika@univ-eloued.dz
University of El Oued

lemouchia-samia@univ-eloued.dz
University of El Oued

Submitted: 02 November 2024 Accepted: 03 January 2025 Published: 29 January 2025

Abstract:

The global trend towards the horizons of digital work has had a major role in the electronic fulfillment process gaining special importance in the recent period, as it is a new system produced by e-commerce that works according to modern electronic mechanisms that did not exist before. Thus, the electronic fulfillment mechanism is one of the most important rights and obligations arising from electronic transactions, but rather a fundamental pillar, if we do not say that this transaction is what led to the emergence of this commitment between the contracting parties, so the concern was for the necessity to define the mechanism of fulfillment on the network itself by means of a bank card, or any method of electronic fulfillment.

Nevertheless, we find that those who shop online often feel insecure about the electronic piracy operations when fulfilling the financial value of the transactions concluded electronically, and then feel that they are not legally protected, and they do not know the truth of their legal status, as is the case with the buyer who deals electronically. So that the feeling of the inability of the other party, who is the seller, to fulfill his legal obligations according to the commercial offer submitted by him. Therefore, the issue of providing the confidentiality of electronic payment card information and thus the security of fulfilling its financial value is one of the obstacles to the growth of electronic commerce.

Key words:Electronic fulfillment; Information security; Electronic risk.

INTRODUCTION

Electronic merchants have become a tangible reality in light of the current commercial environment and the way in which many dealings are made between individuals, from selling and buying goods and services. However, this dealings has imposed challenges and a new reality, which is the reliance on an information system whose tools are all electronic, including payment for fulfillment in this trade, which is done electronically through the electronic transfer of money or shopping with electronic payment cards.

The electronic fulfillment phase considered the necessary customer to be available online to indicate the mechanism for meeting the financial allowance, which is consistent with the peculiarity of electronic commerce and the requirements of speed in it, which imposed this corresponding development in the use of modern and sophisticated means of payment to meet the value of goods and services, which are contracted electronically by the buyer, because of the inappropriateness of traditional means for this type of trade, but the average buyer has become cautious and suspicious while dealing with websites where various commercial offers, for fear of falling into the hands of piracy.

We find that those who shop online often feel insecure about electronic piracy operations, and then feel insufficiently protected legally, and do not know the truth of their legal status, as is the case with the buyer in the electronic sales contract, as they feel that they will not obtain their rights under the contract and do not know the possibility of the other party, which is the seller, fulfilling their legal obligations.

Therefore, the security of data and information in the age of technology has become the biggest role to repel and prevent any electronic attack that may interfere with electronic transactions, and

then protect it from any attempts to access in an unauthorized manner to achieve illegal goals. Therefore, the risks of electronic transactions are the possibility of stealing electronic payment card data, and then the lack of adequate security for the rights and obligations of the parties, especially with the possibility of the buyer being exposed to fraud and fraud, which requires providing protection from them by searching for legal guarantees that would give special protection to the buyer under an electronic sale contract. Therefore, with the spread of this phenomenon, it was necessary to achieve some kind of technical and legal deterrence, as the stability and survival of this system requires the availability of technical capabilities as well as a legislative environment, which supports the safety of electronic payment means in order to instill confidence and spread the spirit of safety in financial transactions between the buyer and the seller.

Therefore, the impact of modern electronic fulfillment mechanisms on the traditional concept of money was the practical step to contain this new reality in dealing, which is carried out in a digital environment through a monetary language commensurate with the digital orientation in the implementation of contractual agreements of a commercial nature. Despite the positive role played by this fulfillment, its implementation raises risks and repercussions that would negatively affect the rights of the parties to the electronic sales contract, especially the buyer. His legal position is affected as a result of hacking websites, obtaining his personal data contained in his bank card, detecting his financial balances, identifying his identity and working to reproduce them, and then using them for illegal purposes. Therefore, it was necessary to search for means and mechanisms to protect him from the dangers he faces when conducting each electronic financial transaction while he is in the process of implementing the electronic sales contract. This allows his transactions to take place in an atmosphere of trust, security and reassurance.

Based on the above, the aspects of this research paper are based on identifying the risks to the means of electronic fulfillment of the buyer, and then exposure to the requirements of electronic means of payment, and therefore the problem can be crystallized in the main question: What are the risks of the buyer fulfilling his financial obligation in electronic transactions? What are the requirements to enhance his confidence in the credibility of the electronic payment mechanism and thus encourage his dealings with it?

We have tried to answer this through two main topics:

The first topic: Aspects of risks to the buyer's commitment upon electronic fulfillment.

The second topic/ Requirements for facing the risks of electronic payment.

Section I

Risks to Buyer's Obligation on Electronic Fulfillment

If the use of electronic payment means has become more than necessary in terms of commercial transactions carried out over the Internet due to their speed and low costs, but practically practicing them has proven the existence of risks that arise and accompany each use of those means, hence the importance of securing electronic payment that ensures trust between the buyer and the seller, as a result of the widespread theft and electronic fraud in the presence of technical persons who have made online theft an excellent source of livelihood. This is what required the introduction of legislative measures to ensure the protection and safe applications, ensuring the rights of users, especially beginners, from the risks that may result from their use of cards or electronic money in settling their commercial transactions. Accordingly, in order to search for guarantees to protect the buyer in order to ensure his safe fulfillment against the risks he may be exposed to during the implementation of his contractual obligation, the study of this topic requires determining the risks of using electronic means of fulfillment in (the first requirement), and then exposure to the objectives of protecting the buyer against the risks of electronic fulfillment in (the second requirement).

The first requirement: What are the risks of using electronic means of fulfillment

The risks arise as a result of the encroachment on the means of electronic fulfillment, especially the bank card, the latter when used through an open information space. The risks that threaten it remain through the circulation of its own data over the Internet, as the Internet receives in an

instant many people from all over the world. This facilitates the penetration of data, which inflicts material and moral damage on the cardholder, or that personal financial information is seized from the card numbers, the name on it, and the due date, in order to use it to seize funds that cover his purchases made online at the account of the cardholder1. Accordingly, the search for the definition of the risks of using electronic means of fulfillment and this in (Section I), and then exposure to the types of risks of using electronic means of fulfillment and this in (Section II)

Section One: Introducing the Risks of Using Electronic Means of Fulfillment

These are the risks that threaten electronic payment methods that appear on the occasion of any electronic transaction, starting from hacking or hacking the database and using it illegally in purchasing and shopping operations or conducting other operations without the consent of the concerned party. The matter may go beyond forging the digital signature and thus its fraudulent use in electronic fulfillment operations, through fraudulent fraud to which anyone may be exposed while in the process of contracting electronically. Therefore, the nature of these risks is multiple and we mention them in this regard, for example, but not limited to, within cases, so we are exposed to them in conjunction with their protection aspects, given the specificity of each case2:

First - Simulation of websites:

It is a case when imitating a real (web) website in its colors, function and subsequent descriptions that distinguish it from other websites that may differ by one number from others3, with the aim of obtaining bank card data or stealing a business, so this case legally includes registering a fictitious electronic domain name that is very similar to a sound sales website, and accordingly4, once an illegal website is created, the drawings of the real legal website are copied, and jobs are created in an effort to imitate links contained in the legal website, so they contribute to providing goods or services at attractive prices in order to push customers to send their bank card data and then acquire them5, this is known as simulating websites.

Protection against simulating websites comes through the mechanism of electronic certificates, because these certificates contain encrypted files that are stored in the website's web server, as these files are connected to the client's browser, and make sure that the site he entered is the intended site. Using these certificates, it is possible to verify the person of the real user connected to the seller's network, so that when this person falls inside the merchant's payment system, the service unit searches for the certificate, and verifies the identity of the person browsing before allowing him to enter6.

Therefore, the electronic card is considered one of the means of verifying the eligibility of the contract upon electronic fulfillment, as all the data of the cardholder such as his name, age, place of residence, bank, and other private data of a personal nature are stored. This card comes as a mobile automated media device that contains a complete record of personal information and data. The card has a secret number that makes it equipped with multiple elements. This ensures the

[1]- Rob Smis et al., **Electronic Commerce, Translation of Tip Top Company**, First Edition, Dar Al-Farouq Publishing and Distribution, Cairo, 2000, p. 229.

[2]- Jalil Al-Saadi, **Problems of Contracting over the Internet**, First Edition, Al-Sanhouri Library, Baghdad, 2011, p. 135.

[3]-This case is also called "fictitious program fabrication", which aims to plan prior monitoring in order to carry out information fraud crimes. Small Jamil Abdel Baqi, **Criminal Law and Modern Technology**, Book 1 Crimes arising from the use of computers, Dar Al-Nahda Al-Arabiya, Cairo, without a year of printing, pp. 49-50.

[4]- Barham Nidal Salim, **Provisions of Electronic Commerce Contracts**, Dar Al-Thaqafa for Publishing and Distribution, Amman – Jordan, 2009, p. 275. Abdel Fattah Bayoumi Hijazi, The Legal System for the Protection of **Electronic Commerce – The System of Electronic Commerce and its Civil Protection, Book 1, Dar Al-Fikr Al-Jami, Alexandria, First Edition, 2002,** pp. 132-133.

[5]-Pauline Antios Ayoub, **Legal Protection of Personal Life in the Field of Informatics,** Al-Halabi Human Rights Publications, Beirut, 2009, p. 148. ForRob Smees et al., op. Cit., Pp. 229-230. And see you Oud Kateb Al-Anbari, Electronic Payment, Journal of the Message of Law, Faculty of Law, University of Karbala – Iraq, Special Issue of the Research of the Seventh Legal Conference, 2010, p. 213.

[6]- Rob Smis et al., op. Cit., P. 233.

protection of the cardholder from forgery and misuse by others in the event of its loss, theft, or attempt to imitate it, which explains and confirms the need for the bank card for effective protection in light of the continuous progress of technology.

Second - Voyeurism on bank card data:

Voyeurism means a case of espionage by reading unprotected data while it is transmitted electronically, which is data of e-mails issued and received from the addresses of the performer of Internet services in order to view and exploit them7, which is an easy process as a result of the use of special programs originally designed to detect Internet errors called (sniffing) programs8, where the voyeur (spy) uses information for his personal account, or sells it to competing companies or professional criminals who use it in thefts9.

This case is subject to special protection against every threat to the electronic payment method in a way that ensures that the data of the bank card traded electronically is not read. Thisis done with the help of a first program, which is encryption, where the bank card data is encrypted by creating a secret code10. This system is dedicated to camouflaging messages and data in a way that is not readable by anyone except the addressee of the secure systems that provide special protection for the confidentiality of the information exchanged in light of the activity of electronic commerce. The second program consists of assistance provided by an information program for the electronic funds archive, which is withdrawn on the electronic card, which is easy to refer to, and this enters the work of the entity in charge of electronic fulfillment online11.

Third - Switching bank card numbers:

This case depends on mathematical systems, so the content of the bank card is changed, and then reconciling account numbers that lead to a specific output that represents the secret number of a bank card circulated online, so the secret number, i.e. the code, is the only guarantee that the bank card will not be hacked, or misused, and here lies the danger12.

Fourth - Illegal penetration of global communication lines systems:

Usually, a customer's computer is linked to that of the merchant through communication lines systems. These systems are hacked in order to obtain the bank card data circulated over the Internet to be used illegally. If it is difficult to determine who carried out this hack, but the method of hacking, its time, and the password used in it can be determined by reviewing the system's access files, as well as its insurance files, to the extent that allows collecting evidence about who carried out this hack13.

V. Technique of destroying the targeted website:

It relies on sending hundreds of thousands of e-mails from one computer to another computer that is targeted, to affect what is known as storage capacity, so that the presence of a huge amount of e-mails will constitute technical pressure, which leads to the bombing of the target site, and thus

---

[7]- Barham Nidal Salim, op. Cit., P. 175.

[8]- "sniffing" means a program for eavesdropping, that is, sensing and taking data from the network through so-called sniffing programs that record all electronic communications between multiple computers. Rob Smies et al., op. Cit., P. 230.

[9]- Oud Kateb Al-Anbari, Electronic Payment, Journal of the Message of Law, Faculty of Law, University of Karbala – Iraq, Special Issue of the Research of the Seventh Legal Conference, 2010, p. 214.

[10]- The secret code is created by first clicking on the password, which consists of different numbers or compound phrases of words that do not exceed 20 words. The program waits for certain moments until the secret code is created, which consists of the card number, type, name of the holder and his phone number, then clicking on the thing that links the code to the party that is interested in online fulfillment. See in this regard the disposition of footnote 02 of: Jalil Al-Saadi,op. Cit., P. 137. See also: Farouk Mohammed Ahmed Al-Basiri, **Subscription Contracts in Internet Databases – An Applied Study of International E-Commerce Contracts,** New University Publishing House, Alexandria, 2002, p. 102.

[11]- Farouk Mohammed Ahmed Al-Basiri, op. Cit., P. 103.

[12]- Abdel Fattah Bayoumi Hijazi, The **Legal System for the Protection of Electronic Commerce,** Book 1, Dar Al-Fikr Al-Jami, Alexandria, 2002, p. 132. Barham Nidal Salim, op. Cit., P. 175.

[13]- Abdel Fattah Bayoumi Hijazi, op. Cit., P. 133.

the scattering and destruction of electronic data stored in it14, so it moves to a computer of those who adopted this method, so that they can roam around it freely, making it easier for them to obtain every information related to the bank card holder in terms of numbers and data15.

This method is often used on the mainframe computers of banks, hotels, restaurants, and travel agencies in order to obtain as many pin numbers as possible for bank cards16.

In addition to the aforementioned cases, there are risks that threaten the bank's function when providing financial services to customers, which would threaten the issue of securing the electronic payment method, as the bank as a financial institution is the largest customer of electronic payment methods, so these risks are added to the risks that every customer can take for this new type of fulfillment, whether a natural or legal person17, as these risks usually occur when banks, within the framework of their electronic payment systems, provide their financial services to their customers, which require going through several stages, so each stage of them is exposed to these risks18.

Section Two: Types of risks of using electronic means of fulfillment

Despite the superiority of man and his acquisition of experience in the field of electronic commerce, when conducting any electronic transaction, he may be exposed to risks that hinder this superiority. This is what appears constantly, especially when he fulfills the value of his electronic transactions, starting from hacking or hacking his bank card database and using it illegally in purchasing, and conducting several online operations without the consent of the concerned party, through forging digital signatures and using them in other electronic fulfillment operations, to fraud and fraud that the cardholder or institutions may be exposed to on the occasion of their electronic

---

14- Pauline Antios Ayoub, op. Cit., P. 149.

15- Emad Ali Al-Khalil, **Penal Protection for Wafa Cards,** First Edition, Wael Publishing House, Amman, 2002,p. 102.

16- An Internet specialist, an investigator in the US Federal Police named John Newton'raised through his author(cart FRQUD) a question that was overshadowed by the exclamation point of what happened to the bank card as a rich topic for organized crime hackers as it is the dream of future generations? As a result, the assets of countries and people become stolen by criminals who base their crime on simple principles in the world of electronics, computers, operating methods and programming, and thus deal with the Internet as a global network? How is a person present in a particular country to be stolen in another country and on another continent? Without a direct meeting between the parties, that is, the physical presence in one council, as the theft is carried out without material damage to the victim? In light of all these questions, John Newton believes that what happens from hacking the electronic card is only a crime of remote theft˙ This is in the world of electronics, the world of remote control, where theft is done by remote control but without control. Imad Ali Al-Khalil, op. Cit., P. 102.

17- Musa Khalil Al-Mitri, **Legal Rules Governing Exchange, New in the Business of Banks from the Legal and Economic** Aspects, Halabi Publications,Beirut,Lebanon,2002,p. 261.

18- These stages are arranged as follows:

- Preliminary stage: At this stage, risks may arise as a result of the issuance of inappropriate decisions during the planning and processing of electronic systems commensurate with the services they provide, as well as that these systems may not achieve what the customer requires.
- The stage of policies and procedures: where the risks arise from administrative negligence and technical inability in relation to electronic activity.

_Internal Security and Control Phase: Risks may arise here as a result of not providing the required internal protection for the information that the bank needs or that is transmitted to it through electronic communication.

_Accounts and Auditing Stage: Lack of auditing and processes used through a particular electronic system would pose a risk to electronic payment methods

- Communication and information systems: Risks arise at this stage as a result of the lack of security with regard to the issue of certification of information received electronically and the inability to identify problems resulting from electronic banks.

contracting19. This is what the Basel Committee on Banking Supervision pointed out, that the electronic banking services provided are not without risks, which requires identifying a policy, management and certain procedures to reduce them, by imposing control over them and thus following them up20. This confirms the role of banks and each legally qualified financial institution through effective planning for their security, based on identifying risks related to computers, the Internet and communication networks. This leads us to research and then identify the types of these risks that the bank may be exposed to when adopting electronic payment systems when settling its financial transactions, the most prominent of which are as follows:

First - Risks of hacking electronic payment systems: The computer system may be accessed by a person who is not authorized to do so, which is considered illegal use, as this work is broken into an original user account and infringes on a digital right, so he performs unauthorized activities, such as modifying application software, stealing confidential data, or destroying files or a specific information system stored for its importance21. A system is usually hacked in the traditional form through covert activities, when the hacker pretends to be the legal person authorized to enter, exploiting weaknesses in a system such as bypassing the necessary control and protection measures in the device, or through information that the hacker gathers from physical sources, such as searching in the private trash can and enabling him to obtain a digital password or information about the system itself22.

Second - Cultivating vulnerabilities: This risk enters a person who is not authorized to do so, or his entry may be legitimate but exceeded the permissible limit, so this entry creates an electronic port and path that enables him to penetrate the device later without the knowledge of its owner, such as using a word processing program that is ostensibly aimed at editing and formatting certain texts, but in the subconscious it represents the real purpose of printing all system files, and transferring them to a hidden file, which enables him to print it and obtain the contents of the system that he has easily penetrated23.

Third - Monitoring and interception of communications: By monitoring communications from one of the communication points or its branches and without penetrating the victim's computer, it is possible for the monitored person, who is the perpetrator, to intercept confidential information that would facilitate his penetration of any information system in the future24.

As for the case of interception of communications, it is one of the risks that are based on the interception of transmitted data by the offender, without penetrating the system, and this is done during the transfer process, when it is modified to suit the goal of the attack, such as the offender creating a fictitious intermediary system that is processed electronically that requires the user to pass through it, which automatically and voluntarily provides the system with sensitive information needed by the offender25.

Fourth - Infringement of the right to license: This is achieved by using a specific system by a person who is licensed for a purpose other than the intended purpose and without obtaining the right to authorize it. This risk is usually highlighted by the employees of the financial institution, as one of them misuses a system, which constitutes an internal danger, which may be external, such

---

[19]- Jalal Ayed Al-Shura, **Electronic Payment Methods,** Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan,2008, p. 87 et seq.

[20]- Jalal Ayed Al-Shura, op. Cit., P. 89.

[21]- Jurisprudence is due to the fact that the reasons for the emergence of risks are due to the possibility of implementing the hacking process from several regions in the world, and to the speed of the hacking process, as it does not need more than minutes to hack and leave the site, in addition to the possibility of sending any message to hack without specifying the name of the sender, which is tampered with to be exploited through some websites online, which makes it more difficult to detect who is responsible for the hacking process. See: Abdel Fattah Bayoumi Hegazy, **The Legal System for the Protection of Electronic Commerce, The System of Electronic Commerce and Civil Protection,** op. Cit., P. 86.

[22]- Musa Khalil Al-Mitri, op. Cit., P. 266.

[23]- Jalal Ayed Al-Shura, op. Cit., P. 95.

[24]- Musa Khalil Al-Mitri, op. Cit., P. 266.

[25]- Jalal Ayed Al-Shura, op. Cit., P. 95.

as using the hacker for the account of a person authorized to use the system by speculating his password, or exploiting the weakness of the system, so he enters it legally and then carries out an illegal activity26.

Fifth -Failure to acknowledge the act: This risk is represented in the failure of the addressee or the sender to acknowledge the act issued by him, as one of them denies the specific signal issued about the purchase or sale of an order he submitted online, or his request for operations from his bank27.

Sixth -Denial of service or commercial transaction: This is achieved when the legitimate user is prevented from accessing information, or obtaining the required service by carrying out activities that prevent this, such as sending an unlimited number of emails once to a specific site, which makes this activity from the system unable to receive this number of messages, so the required service is dropped, in the sense of denying it on its part, or when the person directs a number of addresses over the Internet, which makes it difficult for the system to segment the sent materials according to a certain electronic process, which leads to the server being congested and unable to absorb this number, and then deal with it. Denial of a transaction or business with any institution may also occur electronically, when an Internet user orders a product on a credit line and then transfers it to another site. Upon receipt of the invoice for this commercial transaction, the user may deny issuing an order for this order28.

The risks to electronic fulfillment may be multiplied by multiple reasons, including those due to human and technical factors, without excluding natural risks that are usually from a foreign source, such as natural disasters such as earthquakes and floods, which lead to damage and sometimes destruction of devices related to electronic fulfillment, as well as what may be caused by an electric current interruption or disconnection from the network linking the customer and the electronic fulfillment institutions. This also prevents the completion of an electronic fulfillment process in the best and safest way, or even verifying its completion, whether by the customer or the financial institution. This requires the need to provide alternative electrical devices that withstand the issue of electronic fulfillment from the occurrence of natural disasters that prevent its completion, and then settle financial transactions, and be used by financial institutions practicing electronic fulfillment29.

The second requirement: The objectives of protecting the buyer against the risks of electronic fulfillment

It is logical that containing the risks of electronic payment is achieved through evaluation, control and then follow-up, and this can only be achieved by defining the objectives of protecting the buyer against the risks of electronic fulfillment, as the security and safety of the electronic fulfillment system cannot be achieved without effective security means. This is what makes banks and Algeria Post as legally qualified financial institutions, and distinct in their dealings with contractors holding the electronic payment card approved by them. This is what aims to protect important elements in the field of electronic payment, which are five we list as follows30:

First - Protecting the personal identification of the buyer: Personal identification is one of the means that protect against concealment and disguise activities, so it constitutes an element of protection when verifying identity, especially when the person identifies himself, and the identification is served according to two types. The first lies in identifying the personality and the means of doing so using a secret number, while the second lies in identifying the origin of the information, such as verifying the origin of the e-mail. Therefore, achieving this goal requires the financial institution to make two commitments. The first is the duty to extend its control over each

[26]|||UNTRANSLATED_CONTENT_START|||- مرجعسابق.|||UNTRANSLATED_CONTENT_END|||

[27]- Munir Muhammad Al-Janbihi and Mamdouh Muhammad Al-Janbihi, **Electronic Money,**Dar Al-Fikr Al-Jami, Alexandria, 2007, pp.78-79.

[28]- Waad Kateb Al-Anbari, op. Cit., P. 214.

[29]- Mazouz Dalila, The **Importance of Electronic Loyalty in Evidence and Insurance,**Journal of Knowledge, Akli Muhannad University – Bouira, 10th year, No. 20, June 2016, p. 144.

[30]- Jalal Ayed Al-Shura, op. Cit., P. 105 et seq.

entry into the system to determine the personality of the income earner, and to ensure his financial dealings and his eligibility for that, while the second duty is to stand on procedures sufficient to determine the personality of the customer with the electronic system in order to secure it31.

Second - Protection of access to an information system: Any illegal access to sources of systems, communications and information is prevented, that is, controlling access to the system and extending control over each access. This prohibition extends to include unauthorized access to achieve the objectives of security services, as well as every unauthorized use, unauthorized creation or modification, as well as the destruction or issuance of unauthorized information and orders. Here, security services to control and control access are among the primary means to achieve the right to license it and thus ensure that the owner of this right. This is what requires the financial institution to continuously monitor each entry to the electronic payment system by taking the necessary measures to achieve communication from one system to another, and then closing the field of penetration. Therefore, security efforts must be made to prevent the entry of hackers, which limits their penetration, and to search for certain controls and mechanisms that would reduce the likelihood of risks, whenever the financial institution relies on external sources of a technical nature32.

Third - The element of data confidentiality protection: Confidentiality means hiding information from disclosure to unauthorized parties, and this is achieved through encryption, or through other means that ensure that the size of that information, its source, or the sender is not identified. This requires relying on advanced encryption systems that prevent all authorized access to protected information. If the bank's electronic payment system relies on external technical tools and services that help to extend protection, this requires that the service provider be highly efficient so that it is able to provide a minimum level of electronic insurance with systems that are consistent with what is used in the financial institution and avoid the disclosure of information in a way that preserves its confidentiality33.

Fourth - Protection of the integrity and integrity of electronic content: It is protection from the risks of changing data during the process of entering, processing or transferring it electronically. A secure change process means canceling, replacing or re-registering part of it or otherwise. Protection in this sense includes preventing the total or partial destruction of data or canceling it without a license. Therefore, the financial institution is obligated in this regard to ensure that no modifications are made to customer messages if they are transmitted through electronic channels, and to inform customers of the electronic banking operations used by it, and the method of using them with working on the central data system and monitoring each process individually34.

Fifth - Data transfer protection: It is a protection that would prevent the actor from denying the data transfer or the whole process on its part. This is what falls on the financial institution to maintain direct contact with customers by saving data for digital registration35. It may happen that an electronic system is subjected to a sudden change, technical malfunction, or even in the service provider's system when it is dependent on external elements in protecting against risks arising from electronic payment methods. This is what the financial institution must pay attention to, which holds it responsible for pre-processing by preparing an alternative emergency security study to be used in that case. This is unless the electronic system used by it can do the work required of it, especially when the original system fails to work, which requires the return of the data to the state it was in, or the institution has the ability to provide an alternative system to restart that data, and

[31]- Munir Muhammad Al-Janbihi and Mamdouh Muhammad Al-Janbihi, op. Cit., Pp. 79-80.
[32]- Jalal Ayed Al-Shura, op. Cit., P. 106.
[33]- Sahnoun Mohammed, op. Cit., P. 22.
[34]- Musa Khalil Al-Mitri, op. Cit., P. 270.
[35]- Jalal Ayed Al-Shura, op. Cit., P. 110.

it must work continuously from time to time to operate an alternative system in order to ensure the validity of the system and its ability to work when necessary36.

Section Two

Requirements to face the risks of using electronic payment methods

There is no doubt that electronic payment is the cornerstone of the development of electronic commerce, which means the performance of financial value through electronic means, including credit cards, electronic checks and others. In this digital age, these instruments have the same purchasing power as real money and37 represent a self-contained system.

Jurisprudence defines the electronic payment38 system as"an integrated system of systems and programs provided by financial and banking institutions in order to facilitate secure electronic payment operations. This system operates under an umbrella of rules and laws that ensure the confidentiality of securing and protecting procurement procedures and ensuring that the service reaches the consumer." Through this definition, it is clear to us that electronic payment is a smart system that links three elements together, the communications technology element, the Internet element, and the smart systems element of banks and specialized money companies, in a way that allows customers of financial institutions or money subscribers to exploit their balances in purchases, pay bills, and transfer funds electronically without the need for direct financial fulfillment.

If these means benefit both the seller and the buyer, especially in the field of electronic commerce, but this does not prevent the existence of a risk that may result from their use, which is the possibility of penetrating them and knowing all the information related to the buyer, through their use by other people illegally. This exposes the cardholder's data to theft, which leads to financial loss. This is what prompted many countries to enact laws that take it upon themselves to establish the requirements for the success of the electronic payment system, and then reduce the risks of this fulfillment in electronic transactions through technical and legal mechanisms.

Accordingly, we discuss the requirements for the success of the electronic payment system subject to (the first requirement), provided that we address the requirements for securing the electronic payment system subject to (the second requirement).

The first requirement: Requirements for the success of the electronic payment system

Electronic payment methods represent the most important components of the electronic payment system through which financial transactions take place in a virtual environment. Therefore, electronic payment means a set of electronic tools and transfers issued by banks as a means of payment. Accordingly, electronic fulfillment through these means is considered to facilitate remote transactions between the electronic consumer, who is the buyer, and the electronic supplier, who is the merchant seller, through electronic contracts to complete electronic transactions in which physical and paper means do not appear. This is the characteristic of electronic commerce. Therefore, the establishment and spread of electronic payment means requires basic infrastructure requirements for a technical infrastructure (Section I), and requirements that improve the performance of banking services (Section II).

Section I: Technical infrastructure as a requirement for the success of the electronic payment system

The non-physical aspect of the infrastructure of electronic banks is represented by the elements of the presence of e-mail, web and EDI, as well as HTTP and CP/IP, as well as computers, wires and phones ...And others, and this is for the distribution and transfer of banking information, the establishment of a sophisticated electronic bank characterized by a great demand for its services

[36]- Musa Khalil Al-Mitri, op. Cit., P. 270.

[37] - Salah Zainuddin, **An Economic Study of Some of the Problems of Electronic Payment Methods,**Electronic Banking Conference between Sharia and Law, held at the Chamber of Commerce and Industry in Dubai, from 10 to 12 May 2003, 323.

[38]- Bawadi Mustafa, **Electronic Payment as a Mechanism for Consumer Protection and its Implications in Algerian Legislation,**Journal of Jurisprudence, Issue 14 April 2017, p. 54.

requires the marketing of its website and e-mail and publicity and information about its presence with customers through various means of communication and media.

This confirms that the means of communication and media in turn represent a pillar for the spread of electronic payment technologies, which allow ensuring cost-effective electronic business and secure entry into the information age. On the other hand, the rise of these means of the aforementioned non-physical elements will negatively affect the use of electronic payment technologies. Therefore, the development and continuation of electronic business and ensuring its competitiveness require giving a leading role to the private sector in the field of communication services, and framing an economic policy whose priorities are targeting the telecommunications market through the adoption of a flexible marketing, service and regulatory policy that ensures competition in the market, and then improving the telecommunications infrastructure through organized and effective dissemination, and the optimal and proper use of technical means. This opens the way for the buyer to choose, which increases his social welfare without loss39.

Section II: The need to improve the performance of banking services against the risks of electronic fulfillment

The preparation of qualified and specialized human resources will improve the performance of banks for their banking services, as the development factor in human capital represents a practical procedure through which the individual is provided with a required scientific basis. It is also a technical training process in which the individual acquires specialized scientific capabilities. In addition, it is an administrative organizational process in which management persons are qualified and banking activity is carried out. It is also considered a behavioral process aimed at influencing the behavior of individuals in society. These processes collectively require the adoption of multiple information security strategies40, which proceed from the identification of protection purposes for each electronic payment, which are:

- Confidentiality means ensuring that information is not disclosed or accessed by unauthorized persons.
- Integrity and confidentiality of content, to ensure that the content of the information is correct and has not been modified or tampered with.
- The continuity of the availability of information or service. This means ensuring the continuity of the work of the information system and the continued ability to interact with information.

Banking performance is also related to performance efficiency, which means the good performance of all technical, financial and marketing functions and activities related to electronic banking, as well as working on the objective evaluation of banks' websites through the development of entities entrusted with the task of consulting in the disciplines of technology, marketing and law to assess the effectiveness and performance of their sites41.

The second requirement: Requirements for securing the electronic payment system

Securing electronic banking transactions is very important in the field of protecting the buyer, who is the electronic consumer, and it is imperative that confidence in his acceptance ensures that he is paid for his products or services electronically, so his transactions are settled through electronic banks. Therefore, the latter has the obligation to secure these transactions, and one of the customers may wish to view his information or accounts. In this case, he has to do so using a technical program that is provided to him through a specific system. He is not provided with any information except after verifying his identity and eligibility through this program, and this system

[39]- Mohamed Abdullah Shaheen Mohamed**, Arab E-commerce Prospects**, Dar Al-Kitab Al-Jami, First Edition, 2020, p. 141.

[40]-Refer to: Muhammad Abdullah Shaheen Muhammad**,** op. Cit.,Pp. 143-144.

[41]-Op.Cit;p 144.

acts as an intermediary that prevents any information from falling into the hands of those who do not have the right to it42.

Accordingly, we touch on the guarantees of the protection of the buyer with regard to electronic fulfillment, by researching the requirements for securing the means and methods of electronic payment, in order to instill confidence in these means and accept their use while reassured, not fearing the loss of his money. Therefore, we will turn to the most important mechanisms to confront every breach that occurs on the electronic fulfillment, which provides real protection for everyone who deals in this field, from a technical point of view, which is the subject of (Section I), while we address the protection of the buyer through legal mechanisms in (Section II).

Section I: Technical requirements for securing the electronic payment system

It has become necessary to use means and procedures of an advanced technical and scientific nature that work to secure electronic payments through the transfer of data, with the aim of hiding their content in order to ensure their protection from the dangers of identification, forgery and theft, and thus prevent their illegal modification and use. These include the encryption system, which, along with the firewall, has become one of the pillars of the success of every commercial activity practiced within the field of electronic commerce, and the inevitable necessity in light of information globalization, in addition to what the development of technology has imposed of electronic signature technology as an electronic method, and what is required for its validity of electronic authentication, the latter has become an essential role in documenting electronic transactions, in addition to what has become known as electronic documentary credit as an essential means to meet the price, and all of this can only be achieved by securing confidence in electronic commercial websites, which is what we are initially exposed to.

First: Securing electronic fulfillment by securing electronic commercial websites

The first thing that the buyer deals with in the scope of electronic contracting are those websites where he submits his data to the owner of the site, including the statement of the password of his credit card. This confirms that the secured trade begins with the purchase through a secured site that maintains the data and numbers of credit cards that will be used in the purchase. The buyer will also be able to determine the extent to which the site is considered secure when he sees a metal lock mark at the bottom of the screen in the site where he purchased from.

Therefore, securing the websites of merchant sellers is at the forefront of the guarantees of protecting the buyer while he is in the process of settling his banking financial transactions within the scope of electronic contracting43, based on Articles 8 and 9 of Law44 No. 18-05 related to electronic commerce. It is clear that the Algerian legislator seeks to control the electronic market by framing and regulating the commercial activity under which goods and services are provided and securing their remote circulation through electronic communication. This contributes to securing commercial transactions and electronic payment, which ensures their traceability and transparency in concluding them, which is what the Electronic Commerce Law aims to do in addition to other goals and strategies that this law seeks to enshrine45.

The will of the legislator seems clear when it stipulates two basic conditions for anyone who wants to engage in e-commerce activity and practice this trade. The first is mandatory registration in the

---

42- Bilal Abdul Muttalib Badawi, **Electronic Banks (What they are, their transactions, the problems they raise)**, the work of the Conference on Electronic Banking between Sharia and Law, United Arab Emirates University, held on May 10-12, 2003., p. 169.

43- The term electronic banking transactions means the total financial servicesprovided by banks that rely on electronic data processing, including the effects of electronic exchange of information and processes that govern banking activities.Hazem Naeem Al-Samadi,**Responsibility from Electronic Banking Operations**, 1st Edition, Wael Publishing and Distribution House, Amman-Jordan, 2003, p. 22. See also: Kawthar Saeed Adnan Khaled, op. Cit., P. 605.

44- Law No. 18-05 dated 24 Sha 'ban 1439 corresponding to 10 May 2018, related to electronic commerce, Official Gazette of the Algerian Republic, No. 28 dated 16/05/2018.

45- It is among other objectives that were the subject of research in several citizens of this study, including the protection of the buyer on the occasion of processing data of a personal nature of a natural person.

Commercial Register or in the Traditional and Craft Industries Register, as the case may be. The second is the identification of a website and a bulletin or an electronic page on the Internet. Through this registration, a website hosted by Algeria is opened by adopting an official domain referred to by the legislator according to the extended code (com.dz) with the condition that the website has the means to verify its validity. Then, the person involved is granted a national card because he has become an electronic supplier by the National Center for Commercial Registration. Note that electronic commercial activity is prohibited before registering the type of activity of the seller and his site with the center - a card that is published through electronic communications so that it is accessible to every electronic buyer who can view it, aware of the reality of the person of the seller who deals with it.

Undoubtedly, these conditions constitute guarantees of electronic transactions, which the legislator confirms through Article 49 of Law 18-05 that they must be embodied within a period of six months from the date of publication of this law, which is an obligation that every electronic supplier who wants to practice electronic commerce bears the burden of implementing, in order to protect the buyer in light of this transaction, and factors that inspire confidence and reassurance among Internet users when they realize that they are dealing with a secured site, which in turn reflects on the security of their financial transactions.

This is evidenced by the development of means of protecting the buyer in light of his electronic dealings through the Algerian legislator's endeavor to enhance the transparency of transactions by obliging the previous marking on the merchant seller's Web site (web for its provision of information without misrepresentation, as this would give the buyer the opportunity to verify the guarantees on the site and activate them when necessary[46], as he can click on the access mark to the site of the institution or the presumed commercial store that provides the particular goods or service, and initially identify all the data related to the seller's site, and realize the seriousness of the advanced commercial offer, and reassure him through the transparency of the offer, and thus secure the subsequent stage, which is the stage of fulfilling the value of the place of purchase.

Thus, the security of websites is manifested through their encryption system, so they become secure electronically, and through specialized programs, they are computer programs that direct certain information and instructions to a complex technical device that is stored in the computer[47], in order to prevent hacking and identifying transactions through it. The secured website begins with the letters(https) and not (http), where the letter (s) indicates that this website is secure. This is what the buyer must make sure of before submitting his card number that he is dealing with a secured website, so it is preferable if he wants to shop to do so through those websites, which hide his data, information and credit card numbers before circulating them electronically. These websites are usually symbolized at the beginning of their link with (https) and add the letter (s)as is usual at the beginning of any normal link, which means secure, that is to reduce the chances of infringement cases or what is known as cybercrime[48].

Second: Securing electronic fulfillment through encryption systems

The encryption mechanism allows for the digitization of electronic messages in a way that is not[49] understood by others. This secure system was one of the effective means of securing the buyer's

[46]- Inthis regard, the Tunisian jurisprudence has stated that marking the WAP sites is nothing more than a procedure through which the unreliable, who is not certified, ensures that the product, service or quality system conforms to certain conditions. This explains the transition from the concept of marking to ensure the quality of the product to the concept of marking the WAP sites. See: Asmaa Al-Zalawi, **Consumer Protection in Electronic Commerce,** Master's Memorandum in Contracts and Investments Law, Faculty of Law and Political Science, Al-Manar University - Tunisia, 2009- 1010, p. 73.

[47]- Nazih Mohammed Al-Sadiq Al-Mahdi, **Civil Protection for Computer Programs in Positive Laws**, Proceedings of the Law, Computer and Internet Conference, Faculty of Sharia and Law, United Arab Emirates University, held on 1-3 May 2000, p. 2.

[48]- Jamaleddine Chaoui, **Electronic Commerce Contracts as an Alternative to the Traditional Economy, Legislative and Economic Study**, Dar Al-Numan for Printing and Publishing, Algeria, 2017,p.09.

[49]-Ali Kahlon, **Electronic Commerce,**Journal of Judiciary and Legislation, Tunis, February 2000, p. 27.

electronic financial transactions in the field of its electronic fulfillment50, which is carried out through an information program planned or prepared for the same purpose, representing a secret agreement based on a secret code or key used as an encryption tool51.

Encryption as a system protects the data and information sent through the computers of banks and customers by changing its shape thanks to a code or secret code, so that no hacker of the e-mail can reveal its content and know its content or tamper with it. Accordingly, the encryption system translates an understandable information into an incomprehensible information, through the application of confidential reversible protocols, that is, the possibility of returning it to its original state52, which ensures effective protection of data from any hack or attack when sent over the Internet to the seller's website. This system is considered one of the most important and powerful reliable security and protection systems, especially in securing the electronic fulfillment process that takes place during the commercial transaction. It is used in software called e-wallet. The basis of the strength of this system is to ensure the security of financial transactions by adopting a high-value body called the "Accreditation Commission". This body works to establish an electronic identification unit for both the buyer and the seller in a secured manner after confirming the identity of the buyer as the customer, so that the identity of both of them is preserved and then traded securely and confidentially53.

In this regard, we refer to the set system, the most important electronic exchange insurance protocols that have emerged in the field of electronic commerce, due to its attachment to the most important part of the commercial transactions that take place on the information network, which is the completion of an electronic sale by receiving a purchase order and completing the process of fulfilling the price of purchases over the Internet. This is what made it distinct from other insurance systems with several features. It ensures that the purchase order sent is the same as the order received by the seller with the commercial offer through a certain paper fingerprint that is distinctive to this order. It also ensures the confidentiality of the purchase order by encrypting the information included in the order as well as the data on the fulfillment processes. This ensures the seller that the bank card holder The person wishing to buy is the same as the owner of the account number mentioned in the data sent to him, and also ensures that the buyer's account allows and covers the value of his purchase of the good or service, all without knowing the buyer's bank card number54.

Third: Firewall as a means of securing electronic fulfillment

Due to the importance and value of electronic data at the present time, many other means have been developed to protect it and protect its processing systems, including the firewall, which is one

---

[50]- TheFrench legislator defined through the law of December 29, 1990 the process of encryption as: "All performances intended to transform and assist confidentiality agreements, information or clear signs into information or signs selected for expression or to carry out the reverse operation thanks to the material or informational means established for this purpose." Refer to:Bochurberg (L): Internet et commerce électronique, édition encyclopédie Delmas,1999,P133.

[51]- The decree issued on February 24, 1998 stipulates that secret agreements are monitored as unpublished keys to apply a coded method or performance of numbering or decoding operations. See the legislative development of the cryptographic system in French law in:

-Bochurberg (L),Op.Cit, P P133-134.

[52]- Walid Al-Zaidi, **Online and Computer Piracy**, First Edition, Osama Publishing and Distribution House, Amman, Jordan, 2003, p. 93.

[53]- Theexisting accreditation body, when activating the set system, has several guarantees, including: - Ensuring that the content of the message and the financial information related to it are verified by encryption technology, - Ensuring that the identity of both the seller and the buyer is verified, - Seeking to protect the privacy of the customer by not tracking the quality of his purchases, - Embodying the guarantee of the principle of complementarity, indicating that the message sent is the same as the message received. See: Nader Shaaban Ibrahim Al-Sawah, **Plastic Money and the Impact of Electronic Transactions on Internal Audit in Commercial Banks**, University Publishing and Distribution House, Alexandria, 2006, p. 124.

[54]- Diaa Ali Ahmed Noman, op. Cit., P.29.

of the non-physical security means used in turn to secure private networks from entry, preventing illegal access to it inside the network, where it protects the control and transmission units in the Internet55. It is defined as a set of information systems and programs that provide security fences between the Internet and the network of the institution or the electronic government, forcing all transits on the network and exit from it, and to pass through the firewall that repels intruding users from accessing the network. "56The importance of this means is evident as a protection system for the front wall of the customer's computer, which works to prevent snooping, that is, spying on personal information, so it preserves the personal computer and that is the channel used by the computer from snooping through other channels or programs, especially the open Internet57. Thus, the firewall is one of the technical methods to protect the integrity of information, by technically repelling every intruder or professional user, allowing the creation of a secure network between the Internet and the organization's network, so that it is safe from illegal intrusions58.

Fourth: Securing electronic fulfillment through the electronic signature system

The electronic signature is one of the guarantees of the protection of the buyer in the field of electronic fulfillment, as this system is used to sign letters addressed to his bank, as well as to sign fulfillment orders addressed to his bank, and the legal regulation, protection, authentication, and evidence received by the electronic signature59.

In this regard, we point out that what is placed about the electronic editor and takes the form of letters, numbers, symbols, signs, or others, has a unique character that allows the identification of the person of the signatory and distinguishes him from others. The mechanism of the electronic signature is done through a specific form, so that it performs two functions. The first is to prove the identity of the signatory, and the second is the ratio of the behavior that the signature carries to its owner. This authentication system is used in the scope of financial transactions, as it leads to the verification of the person of the signed customer and the percentage of the signed message to him, so no one can manipulate this signature and then the encrypted message, this confirms that each customer has his own signature that does not resemble another60. The electronic signature can be used to protect the customers of banks who use electronic checks to complete electronic

---

[55]- In addition to the non-physical means of information security, there are physical means aimed at preserving computers and their accessories and the necessary protection for cylinders, tapes, printers, storage and communication places, which is achieved in practice by providing tangible defense security to protect facilities from accidents, natural disasters and intentional damage. See on that: Tamam Shawky and Khalifa Mohamed, Automated Data Processing System as a Basis for Penal Protection in Algerian Legislation, Journal of the Generation of In-depth Legal Research, Center of the Generation of Scientific Research, Tripoli - Lebanon, Third Year, Issue 25, May 2018, p. 19.

[56]- Diaa Ali AHamad Noman, op. Cit., P. 39. Also: Hijazi Abdel Fattah Bayoumi, **Electronic Government between Reality and Ambition**, First Edition, Dar Al-Fikr Al-Jami, Alexandria, Egypt, 2008, p. 220.

[57]- Waked Youssef, The **Legal System of Electronic Payment**, Master's Memorandum in Law, Public Law Branch, Faculty of Law, Mouloud Mamari University, Tizi Ouzou, 2011., p. 170.

[58]- See more detailed about this technical method: Ghaniya Batali, **Cybercrime – A Comparative Study**, Algerian Publishing and Distribution House, Algeria, 2015, p. 141 et seq.

[59]- This is what was decided by French Law No. 230 of 2000 issued on March 13, 2000 to adapt the law of evidence for information technology and electronic signature. Before the issuance of this law, the French judiciary recognized the validity of the electronic signature and its authority to prove it. See Kilani Abdel Radi Mahmoud, The **Legal System of Loyalty and Guarantee Cards**, PhD Dissertation, Faculty of Law, Ain El Shams University, Egypt, unpublished, 1996, pp. 184-185.Huda Hamed Kashkoush: **Criminal Protection of Online E-commerce**, Cairo, Dar Alnahda Alarabiya 2000, p. 71 et seq.

[60]-There are many formsof electronic signature, where we find what is used in the operations of banks andelectronic payment in general, which is the signature code, andthere is the biometric signature**,** which depends on the physical and behavioral characteristics of the person, and the digital signature, which depends on encryption and linking it to private keys to decrypt.See Ibrahim Al-Desouki Abu Al-Lail,**Documentation of Electronic Transactions and the Responsibility of the Documentation Authority towards the Affected Third Party - Legal Aspects of Electronic Transactions**, Kuwait University, Scientific Publishing Council, 2003, pp. 1853 et seq.

payments with other parties. The bank acts as an intermediary after writing the check with the customer's signature electronically, encrypting the check and then sending it to the bank. The latter solves the code and verifies this signature and then records its value on the customer's account and adds it to the account of the other party61.

Fifth: Securing electronic payment through the electronic documentary credit mechanism

The idea of documentary credit was an old idea, but the technological progress in the field of commercial transactions has called for the adoption of a mechanism that links the seller's implementation of his obligation to deliver the commodity or provide the service with the buyer's implementation of his obligation to pay the62 price. It is a procedure that depends on the work of banks because of the material and technical capabilities they have. The emergence of the so-called "electronic documentary credit" through which all previous procedures and messages63 are carried out, whether between financial institutions between them or between them and the parties to the accreditation process in an electronic manner. Thus, the documentary credit is one of the most important results of the development in electronic communications technology64.

This mechanism is based on the use of documents issued on the occasion of the implementation of the sale contract based on the buyer's will to contract for a specific commodity, so it is agreed to pay for it through a documentary credit, so the buyer goes to his bank and requests to open a credit in favor of the seller specifying everything related to the sale and its conditions, including that the payment of the price is not made until after the expiry of the legally prescribed period of return. The bank shall inform the seller of this credit opened in its favor, ordering it to send the commodity to the contracted party with the same specifications. Then, the calculation of the time limit for withdrawing from the contract begins from the date of the buyer's receipt of the commodity. This imposes on him at the end of the period that the buyer notifies both the seller and the credit-opening bank of his final opinion, either to continue to buy holding the commodity and implement the sale, until the bank meets the agreed price to the seller, or to withdraw from the purchase and the amount is returned to him, after making sure that the seller recovers his commodity65. With this banking procedure, the buyer guarantees that the value of the sale has not been paid, and it did not reach the seller until after the end of the period prescribed for its own benefit to exercise its right to withdraw from the purchase. This also constitutes a guarantee procedure for the seller to secure its right after the end of the period of withdrawal when the buyer's position is positive. It also protects it against fraudulent orders or those made under a false name or through which the buyer intends to manipulate it66.

In the electronic sales contract, the seller may require the buyer to open a credit for him by a certain bank that undertakes to fulfill the value of a certain documentary credit once he submits documents related to the commodity that conform to the conditions of the credit. This is done under the electronic documentary credit, where the buyer sends his request to open this credit to the bank. If he receives approval, its content is sent to the buyer, and then the beneficiary seller - after being informed of the opening of the credit - sends the documents related to the

---

[61]- Hisham Fathi Sayed Hussein, **Means of Electronic Consumer Protection between Sharia and Law**, Proceedings of the Conference on Electronic Banking between Sharia and Law, Faculty of Sharia and Law and Dubai Chamber of Commerce and Industry, United Arab Emirates University, held on 10-12 May 2003, p. 1203.

[62]- Kawthar Saeed Adnan Khaled, op. Cit., P. 616.

[63]-Hussein Shehadeh Al-Hussein, **Electronic Documentation in Documentary Credit,** Proceedings of the Third Scientific Conference of Egyptian Laws held at the Egyptian Society of Law, Economics and Legislation under the topic "Legal Aspects of Banking Operations", Cairo on 19 and 20 December 2002, pp. 1and beyond.

[64]- Bilal Abdul Muttalib Badawi, op. Cit., P. 1959.

[65]-According to this process of documentary credit, jurisprudence defines it as: "A credit opened by a bank at the request of one of its customers in favor of another person by guaranteeing documents representing movable goods or intended for transport." Mahmoud Mukhtar Ahmed Breary, **Commercial Transactions Law – Banking Operations**, Dar Al-Nahda Al-Arabiya, Cairo, 2004, p. 136.

[66]-Mahmoud Mukhtar Ahmed Breary, op. Cit., P. 137.

implementation of the sale that are necessary to disburse the value of the credit to the bank via e-mail, in the same way that the request to open the credit was sent provided that the credit remains valid67. When the bank confirms that the documents sent by the seller conform to the terms of the credit, it shall pay to the seller the value of the credit opened with it, by electronic bank transfer, after which it shall be credited to the buyer's bank account68.

Based on the above, the establishment of the mechanism of electronic documentary credit through a special legal regulation will undoubtedly constitute a legislative guarantee that guarantees the protection of the buyer within the scope of electronic fulfillment, as it allows the buyer to exercise his right to renounce without fear that he will recover the price he paid if he returns from the purchase, indicating that this credit gives him a right not to pay in advance before the expiry of the period of reflection legally granted to him under the right to renounce the sale. On the other hand, it also represents a guarantee for the seller, as it allows him to deal without fear of procrastination by some buyers, whether in paying the price when executing a sale, or returning the commodity in its condition when the buyer withdraws from the purchase.

Section Two: Legal Requirements for Securing the Electronic Payment System

They are legal conditions stipulated under the text of Articles 28 and 29 of Law No.: 19-05 related to electronic commerce required by the Algerian legislator to use electronic payment. They are considered one of the legal requirements to confront any risk that the buyer faces when fulfilling the financial value when contracting electronically, which is that the electronic payment must be secured through the electronic certification system, and that the electronic payment is subject to the control of the Bank of Algeria.

First: Securing electronic fulfillment through electronic authentication

The increasing risks of e-commerce in light of the development of technical programs that help to penetrate the privacy of people and their financial transactions over the Internet, has had an impact on the emergence of modern means, including the adoption of a third person mechanism as a reliable party to ensure the integrity of the transaction between the two parties69, representing a certain entity that confirms the validity of each transaction carried out over the line by providing a certificate proving this, confirming the validity of information related to payment, maintaining the confidentiality of data exchanged over the Internet, in addition to verifying the validity of the smart card and the availability of credit to allow for the fulfillment of a certain value70. If the electronic signature is a real guarantee for the parties to the electronic transaction, it is not so unless it is an electronic authentication. Electronic authentication is one of the legal guarantees to prove the validity of the electronic signature and thus the validity of electronic transactions, including the electronic sales contract.

Electronic authentication has been defined as "a technical legal process aimed at proving that electronic messages and signatures are issued by those to whom they have been attributed, without misrepresentation, forgery, or forgery carried out by an independent neutral party, who issues an electronic certificate that achieves the desired purpose71." Thus, the basic functions of electronic authentication are clear, and its adoption of a technical mechanism to protect financial transactions, as it guarantees the factor of trust and security in the electronic sales contract by proving the identity of its parties, and determining the truth of what they agree on and its content.

67- Kawthar Saeed Adnan Khaled, Electronic Consumer**Protection**, New University House, Alexandria, Egypt, 2012, p. 617.

68- Hazem Naeem Al-Samadi**,Responsibility from Electronic Banking Operations**, First Edition, Amman, Wael Publishing and Distribution House, 2003, pp. 68-70.

69- Moncef Kartas, **Electronic Commerce and Applied Problems**, Journal of Judiciary and Legislation, Tunis, July 1999, p. 40.

70 -GUICHARD(S), M.HARICHAUXet DE Tourdonnet (R), Internet pour le droit , Montchrestien, 2ème édition, Paris 2001, P 231.

71- Drees Kamal Fathi, **Electronic Authentication Mechanism as a Guarantee for Commercial Transactions by Modern Means in Algerian Legislation**, Journal of Research and Studies, Martyr Hama Lakhdar Universityeloued, Issue 24, Year 2017, p. 162.

It also guarantees the confidentiality of data as the authentication function is related to encrypted writing technology, which achieves a link between the principle of confidentiality and the authentication system72.

The concept of certification can be deduced from what was stated by the Algerian legislator in accordance with Law 15-04, which defines the general rules related to electronic signature and certification, as electronic certification was defined only when it dealt with the term electronic certification, and it was defined within the provisions of Article 02 of the above law in the seventh paragraph73.

The term"electronic certification services performer" was also used and defined in paragraph 12 of Article 2 of the aforementioned Law 18-05, and the legislator intervenes again from the same law74, so it adjusts the rules of work with electronic certification within the provisions of Chapter Three, when it stipulated the electronic certification certificate described in Chapter One of it and this is in the text of Article 575, which are certificates granted by the electronic certification services performer, so his intervention is limited to ensuring the relationship between the signature and its owner without interfering with the content of the certificate76.

Therefore, in order to ensure the safety of electronic payment, the buyer is required to provide the intermediary in the transaction with his bank card number and account number in exchange for obtaining his own ID number. In this case, the intermediary initiates the payment process instead of the buyer, who then delivers his ID number to the seller and is able to obtain his financial dues with the trusted third party. If this process provides sufficient guarantees for the safety of the transfer of funds and their access, the guarantee must be entrusted to financial institutions that are legally qualified to do so, and they are responsible for maintaining the buyer's balance and ensuring that the amount reaches the seller or service providers, which ensures the transparency of the transaction.

The legislator always emphasizes the importance of the electronic certification system as a basic guarantee for electronic transactions in general, and for electronic commerce in particular in order to achieve the requirements of trust and security as stated in the provisions of Article 28 of Law 18-05 related to electronic commerce within the provisions of Chapter VI entitled " Payment in Electronic Transactions", which states that: "The connection of the Internet site of the electronic supplier to the electronic payment platform must be secured by an electronic certification system."

It is clear from the text the role of the authentication certificate as a document that would secure every financial transaction through the payment platform, and the electronic certificate is considered secured through the electronic signature of the person who issued it and through which he attests, after the inspection of the validity of the data it contains, this is what the Algerian legislator expressed through the previous legal text in the word Wasl of the seller's Internet site, which is issued and is secured through the certification system, so that this receipt serves as a document or certificate of authentication that documents and guarantees the financial transaction,

[72]- Drees Kamal Fathi, op. Cit., P. 163.

[73]- The seventh paragraph of Article 02 stipulates that: "The following means:...7- Electronic Certification Certificate: A document in electronic form proving the link between the verification data of the electronic signature and the signatory..."

[74]- Paragraph 12 of Article 02 reads as follows: " ... – Performer of electronic certification services: A natural or legal person who grants described electronic certification certificates, and may provide other services in the field of electronic certification."

[75]-Article 15 of Law 15-04 was included in the provisions of Chapter One on the electronic certification certificate described in Chapter Three, entitled Electronic Certification, where the legislator indicated throughit the nature of this certificate by the availability of certain important requirements that must be met init and the data it must contain.

[76]- Ali Kahlon, **Informational Responsibility – An attempt to control the advantages of the responsibility of those involved in the framework of informational applications and services**, University Publishing Center in Tunis, 2005, p. 390.

so the connection of the electronic service provider's website to the electronic payment system is secured through the electronic certificate issuance system77.

Based on the text of Article 29 of Law 18-05 and in order to78 ensure the requirements of interoperability, confidentiality, integrity and security of data exchange, the Algerian legislator subjected the electronic payment platforms that were allocated for this purpose, where the value of the goods and services subject to electronic transaction is fulfilled by the buyer to the control of the Bank of Algeria. This also ensures that the buyer's funds are safe because his financial transaction was secured by that control, which ensures that his account balance is not manipulated and that his online financial transactions are directed to their beneficiaries.

Second: Securing electronic fulfillment under the security of payment systems

The banking policy in Algeria has worked to ensure the security of electronic fulfillment through the issuance by the Bank of Algeria of Regulation No. 05-0779, which includes the security of payment systems. This regulation defines the interbank payment system or the settlement and delivery of financial instruments as national or international procedures that regulate relations between at least two parties that have the status of a bank, financial institution, or institution involved in the clearing house80.

According to Article 04, paragraphs 1and 2 of Law 05-07 related to the security of payment systems, this system is mainly based on ensuring the infrastructure of multiple payment systems and means, which concerns the infrastructure of the central components to produce technical equipment or software placed at the disposal of accredited subscribers, and the effectiveness of the process for the infrastructure, especially with regard to communications and electrical energy.

Article 05 of the same system stipulates that the infrastructure of payment systems includes, in particular, "the availability of systems, the validity of mutual data, the drawing of the scheme of mutual data, confidentiality, and reviewability." In accordance with this Law, the Bank of Algeria is also keen, through the text of Article 12, paragraphs 1and 2 of the aforementioned Law 05-07, to provide physical and logical security for the infrastructure of payment systems. It also makes sure that the security of means of payment is provided without monetary currency, and that applicable standards are respected in this field. When the Bank of Algeria considers that one of the means of payment does not have adequate security guarantees, it may request the issuing authority to take appropriate measures to address the matter. In the absence of application of these recommendations, the authority in charge of monitoring shall be consulted to take the decision to suspend the entry of a specific means of payment into the system. On the other hand, the payment systems security system, according to the text of Article 12 in paragraph 3, obliges the Bank of

---

77- The Regulatory Authority of the Post and Transport in Algeria initiated the preparation of a project on the electronic certificate on securing transactions through the transport network, related to the organization of an open national and international tender on 06/09/2009 to find a company specialized in the field of electronic certificates, which is mainly tasked with developing the tools and mechanisms necessary to establish and follow up the use of electronic certificates during the exchange of data over the Internet, as the card user can conclude transactions online and pay for the purchase of online collectibles from merchants, in a secure environment against fraud and piracy, thanks to the circulation of encrypted information as well as the use of a personal access code that helps to verify the identity of the cardholder. See: Wadi Yousef, op. Cit., P. 182. Also: Dimish Sumaya, **Electronic Commerce: Its Imperative and Reality in Algeria**, Master's Memorandum in Economic Sciences, Faculty of Economic Sciences and Management Sciences, University of Menturi, Constantine, 2010-2011, pp. 266-267.

78- Article 29 states the following: "Electronic payment platforms established and exploited, in accordance with Article 27 above, shall be subject to the control of the Bank of Algeria to ensure that they meet the requirements of interoperability, data confidentiality, integrity and security of exchange."

79- Regulation No. 05-07 dated 26 Dhu al-Qa 'dah 1426 corresponding to 28 December 2005, including the security of payment systems. Official Gazette of the Algerian Republic No. 37, issued on 04/07/2006.

80- This is stipulated in Article 02 of the aforementioned Payment Systems Security Law. He reviewed: Abdul Raouf Dabbash and Zabih Hisham, **Means of Payment between the Technical and Legal Protection of the Electronic Consumer**, Journal of Jurisprudence, issued by the Faculty of Law and Political Science at Mohamed Khader Biskra University, No. 14, April 2017, p. 116.

Algeria, being the legally qualified and exploited institution, to ensure the security of payment cards, follow up the procedures for providing security conditions carried out by the issuing authorities, as well as traders, and follow up on fraud statistics and developments in the fields of technology that may affect the security of payment cards.

In this context, the Algerian legislator was keen to ensure electronic fulfillment by issuing Law 18-04, which specifies the general rules related to electronic mail and communications81, when it subjected the activities of the electronic mail and communications sector to state control82, as the effectiveness of this control appears when transferring funds through all means of written or electronic payment, as Algeria Post is responsible for the funds it receives electronically transferred to it, which is due in a special credit for postal accounts, until it is paid to its beneficiaries within the conditions prescribed in the regulations83.

Conclusion

In this research paper, we conclude that e-commerce has provided the opportunity to search for and buy goods and services through an information network, where it is possible to sell and buy through websites similar to commercial centers. The Internet has become an effective tool in displaying, marketing and advertising the product, turning it into a new display and carrier interface for trade, and a means of exchanging data. It has also made contracting in order to exchange what is offered remotely from sales a tangible commercial reality, starting with the relationship of the merchant seller as an electronic supplier with the buyer as an electronic consumer through the application of the sale and receiving it through technical means within the digital information environment to the electronic payment. In light of all this, the study addressed an important problem on the extent of guaranteeing the rights of the buyer as an electronic consumer and protecting it when fulfilling the value of its electronic transaction.

The combination of digital systems with the practice of commercial activities has had a great impact on the legal systems becoming coupled with the requirement of full and integrated protection for the buyer as an electronic consumer. This is what we stood by byby analyzing the provisions of Law 18-05 related to electronic commerce. When regulating this activity, the Algerian legislator focused on the rules dedicated to the effective and safe protection of the electronic consumer at all stages of the contract under obligations that the seller bears the burden of implementing as an electronic supplier. Therefore, the challenges raised by information technology and communication technologies have affected legal relations, including primarily the person of the buyer as an electronic consumer, who finds himself, especially with the complexity of transactions, exposed to risks to his security, safety and confidentiality of his data, which necessitates the provision of a legal framework that guarantees his trust and security in a way that preserves his rights arising from the electronic sale, which relate to ensuring the implementation of his obligation arising from the contract, and therefore it was to reach results, and the resulting recommendations from us that we address successively:

CONCLUSION:

The availability of security and safety elements in the electronic payment system comes at the forefront of the guarantees that must be available when the electronic payment process, and therefore the availability of confidence and safety of the parties to the process from users and dealers of electronic suppliers.

The supervisory and supervisory role of the Bank of Algeria as a financial institution on electronic payment based on the requirement of electronic platforms and the requirement of electronic certification, which helps to establish an effective legal system for the electronic payment system.

81- Law No. 18-04 dated 24 Sha 'ban 1439 corresponding to 10 May 2018, specifying the general rules related to mail and electronic communications, Official Gazette of the Algerian Republic No. 27 dated 13/05/2018.

82- See the text of Article 03of Law No. 18-04 specifying the general rules related to mail and electronic communications, op. Cit.

83- See Article 46, paragraph 04, and Article 57, paragraphs 1and 3, as well as Article 62, paragraph 1, of Law No. 18-04 specifying the general rules relating to mail and electronic communications, op. Cit.

The Algerian legislator's interest in the issue of the security and confidentiality of electronically circulated information began with the issuance of the Electronic Signature and Certification Law, as well as the Electronic Commerce Law, but it recorded a delay in issuing legal regulations that enshrine the general provisions of the legislator that singled out electronic transactions in their aspect of financial fulfillment.

RECOMMENDATION:

1- We propose the enactment of regulatory texts by the legislator, the subject of which is the establishment of an administrative body to undertake the task of granting the license and monitoring the commercial advertisements contained in the offers submitted by the sellers through the websites, and authorizing them with all the necessary powers, so that these advertisements come in line with the desired purpose of publishing or broadcasting them in terms of determining the exact nature of the false or misleading commercial advertisement, and making it absorb the cases of refraining from providing data that it was important to inform the consumer about, given their great impact on proceeding to contract. It also works to prepare effective controls that would regulate the advertisements that are broadcast on the Internet, especially those that sell services, goods and products at the national level, and to develop mechanisms to alert Internet users of false advertisements and show how to ensure their sincerity. This regulation, when it ensures that it is dedicated to that body, constitutes recognition of the advertising message with a legal value as it represents a positive. This results in the contractual responsibility of the advertiser as an effect of his failure to fulfill what he stated, which is the electronic supplier. As well as what can be performed by that administrative body to ensure that each consumer is periodically informed of all the necessary information about the goods and services offered in the market and ways to use them and ways to prevent damage.

2- Due to the total reliance of the electronic payment system on electronic means through which the payment and transfer processes take place, and once these means are developed, the laws that sponsor traditional payment systems do not apply to them. We charge the legislator with the need to draft special laws and texts that regulate electronic payment methods in general and electronic money in particular and protect their customers, in addition to clarifying the methods of dealing with electronic money and regulating the issues resulting from them, including determining civil and criminal liability in the event of their illegal use, whether by their owners or third parties. This leads to solving the problem of legal protection of electronic fulfillment by adopting a holistic approach that takes into account the attention to the legal framework through the enactment of legislation on electronic banking operations, in order to accommodate all developments in all transactions on the one hand, and to involve banks and financial institutions in the preparation of laws related to electronic fulfillment systems in order to reach sound legal formulas on the other.

3-The importance of the role of the banking sector in building human cadres familiar with these modern means, in order to deal with electronic payment means in a conscious manner that helps in the progress and utilization of banking services, which contributes to securing electronic financial transactions for the buyer.

4- We also hope and call on the Algerian legislator to find a mechanism that links the seller's implementation of his obligation to deliver and the buyer's obligation to pay the value of his purchases, which is the electronic documentary credit, which he deals with by a special regulation for the means of securing electronic fulfillment and thus a special legal guarantee for the buyer under his contract of electronic sale, which is a mechanism as we have seen based on documents issued on the occasion of the implementation of the electronic sale contract, according to which the seller requires the opening of a bank credit that undertakes to fulfill the value of the credit once the seller submits documents that prove the nature and existence of the commodity and conforms to the conditions of the credit, once the bank confirms that the documents conform to those conditions, it fulfills to the beneficiary seller through an electronic bank transfer that is then credited to the buyer's account.

5- Despite the Algerian legislator's endeavor to achieve speed in the transactions that take place in the field of electronic commerce, and the replacement of traditional electronic bonds, by providing an electronic certification mechanism as a guarantee for the parties to the electronic contract, we therefore urge the need to work to accelerate the process of establishing the bodies in charge of electronic certification.

6- We also suggest issuing a special payment card to buy online, and in addition to the card number, a special code is used to identify the holder, which is the electronic consumer whenever he uses it, so that if the websites are hacked, and the card numbers are not used.