

ELECTRONIC FRAUD FROM CHANGING THE CONCEPT TO CHANGING THE PROTECTION

Ghazioui Hinda*

University of 20 Ougust 1955 Skikda- Algeria-

ghazioui_hinda@yahoo.com

Date de soumission

Submission date

30/08/2023

Date d'acceptation

Acceptance date

28/12/2023

Date de publication

Publication date

31/12/2023

Abstract:

Fraud and swindling are considered traditional crimes that are based on appropriating movable money owned by deceiving the victim and forcing him to hand over, and the Algerian legislator stipulated it in article 372 of the penal law, have evolved in the information era and the term "electronic fraud" has emerged, as the crime takes place on digital platforms aimed at seizing others' money using various fraudulent ways. Recent instances, such as the fraud experienced by Algerian students studying abroad, highlight the urgency of addressing electronic fraud in legal frameworks, and the challenges posed by electronic fraud on virtual platforms, seeking to determine whether reliance on traditional legal texts is sufficient or if new measures are essential for effective protection against these specialized crimes and accordingly came this study to shed light on the concept of electronic fraud from the concept transformation leading to the need to redefine protection mechanisms.

Key words: Fraud; swindling, electronic crime; protection; penal law; virtual world).

Introduction:

Traditional Fraud is defined as appropriating the money of others by deceiving the victim and forcing him to hand it over, but this concept has changed in light of the current technological development, especially in the face of the technological revolution and the use of the world wide web in most activities and services of modern communication devices, so that computers and mobile phones occupy the important place in the new life which resulted the dangers and illegal uses of information technology wither it affected digital data, personal accounts, or service websites, so new term appeared ,which is electronic fraud .

Electronic fraud is the new type of electronic crime, which is through the virtual space, it has occupied the forefront and is now competing with

* Corresponding Author

traditional crime, as a result of the rapid use of technology and means of communication that no one can do without because of their necessity, and electronic fraud has become the most prevalent among individuals and companies, due its characteristics, virtual transaction are mostly transactions with unsecured results, and transaction take risks when the result is the delivery of exorbitant money in exchange for the fraud and deception of the information criminal . But on the other hand, this use contributed to illegal uses and electronic crimes appeared that crossed national borders, comparable to traditional crime .which beats the alarm in order to flight or combat it .

Algeria, like other countries worked to up in place an integrated legal system that protects the rights of dealers through the internet network from electronic crimes in general and fraud in particular, given that the victim is an ordinary person, who does not have experience and competence in the field information, and given that the Algerian legislation did not provide special texts criminalize electronic fraud, as well as obligatory return to the general rules that criminalize the fraud stipulated in article 372 penal law, also return to law n ° 09/04 that includes special rules for preventing and combating crimes related to information and communication technologies, and the criminal procedure law was amended in 2021, law n°21/11 that included establishment a pole specialized in electronic crimes .

The objectives of the study:

- Clarifying the concept of electronic fraud and the need to combat it through new texts dealing with how to prevent it, how to combat and criminalize it.

- A study of electronic fraud between the traditional and new concept .

The problem raised: on all the previous data, we had to raise the following problem: what is the concept of electronic fraud between its traditional meaning and the new meaning? And what are the ways to change the means of protection from cybercrime?

The answer for this problem, we have to adopt the analytical approach, through analyzing texts that have contributed to addressing electronic fraud both in public rules and in special laws.

In addition to adopting the descriptive approach by describing the phenomenon of electronic fraud and its features.

Which forced us to adopt a bilateral plan in order to deal with the elements of the subject as follows:

- 1 –The concept of electronic fraud and its features.

- 2 – The need to change the traditional protection mechanisms.

1 –The concept of electronic fraud and its features.

Electronic fraud is a form of fraud in general. So, the concept of electronic fraud should be addressed and then exposed to its distinctive features:

1 –1 the concept of electronic fraud:

It is a necessary to address the linguistic meaning of fraud and then the terminology.

- Linguistic meaning:

Fraud means the language of asking for a trick, a source of fraud defrauding his friend and he took his money from him, arranged a trick for him ⁽¹⁾ just as fraud know the language of staring at managing matters ⁽²⁾.

The origin of deceit is from squint, deceit, transformation and deception sharpness, quality of sight and the ability to act ⁽³⁾; and it was said that the trick means stare at managing things and it is the predominance of through until it is guided to the intended its origin is way, and it is a fraud to ask for a trick ⁽⁴⁾.

- Fraud in the French language means swindle *l'escroquerie*, on the ground that its deception that is carried out by fraudulent, means such as using false names or delusional qualities or fraud with the aim of receiving the money of others ⁽⁵⁾.

- Terminological meaning:

Fraud is defined within the scope of criminal law as an illegal act emanating from a criminal will for which the law determines a penalty or a precautionary measure ⁽⁶⁾.

- The French legislator considered the fraudster an artist and genius acting in order to catch his prey ⁽⁷⁾. fraud is one of the forms of crimes involving money, and it is one of the traditional and advanced crimes at the same time, but it has acquired a distinctive character, because of the elements and behavior foundations on which it is based and an image that express personal characteristics based mental work, innovative sophistication and the skillful capabilities of the perpetrators of these crimes, in addition to behavioral ability that fraudsters possess today, which is represented in disregarding laws and instructions, and the crime of fraud is one of the methods of organized crime, rather it is the most important method of its method, as all crimes fraud or forgery ⁽⁸⁾.

- In the world of computers, fraud of a special kind has appeared with its own characteristics and features, the internet is the distinctive means for a criminal to commit his crime .It consists of a series of behaviors .Such as modifying or deleting data, stealing files, or changing systems and programs .Fraud is also used for extortion and fraud.

And there are those in jurisprudence who gave the name fraud to the meaning of escroquerie, as escroquerie was defined as the seizure of movable and owned money by deceiving the victim and forcing him to hand it over⁽⁹⁾.

- You also find the definition of swindling as the international taking of full possession by fraud⁽¹⁰⁾.

- The crime of swindling was also defined as appropriating the money of others using fraudulent methods that in the delivery of money to the accused, including the Algerian in article 372 of penal law⁽¹¹⁾, as it stipulated that anyone who reached or received money, movable, bonds, disposals or papers financial, promises, clearances release from obligations, obtaining any of them, or attempting to do, so and that was by fraud to take away all or some of the wealth of others, or attempting to do so, either by using false names or adjectives, or imaginary authority or financial dependence, or by events in the hope of winning anything, or in the occurrence of an accident or any other imaginary incident, or the fear of something happening there of shall be punished by imprisonment from at least one year to five years at most, and a fine of 20.000 to 100.000 DA.

- It is noted that despite the difference of researchers and jurists about the different meaning between fraud and swindling, it is agreed that fraud are two sides of the same coin, and is the same orientation of the Algerian legislator who stipulated the crime under the heading of swindling and linked the conditions for committing it to the use of fraudulent. And the French legislator who used the term "escroqueries", which includes those concerned together⁽¹²⁾.

- In the world of computers fraud of special kind has appeared with its own characteristics and features. Internet is the distinctive means of a criminal to commit his crime, it consists of a series of a behaviors such as modifying or deleting data, stealing files, or changing systems and programs, fraud is also used for extortion and fraud to seize the money of others, which is known as electronic fraud, which is based on using fraudulent methods stipulated by law to seize the money of others.

New crimes, therefore the concept for electronic fraud has been linked to the general concept, for electronic crime that is caused by the illegal use of the internet or is every activity in which electronic technology is used as a means to implement scheme⁽¹³⁾.

1 – 2 characteristics of electronic fraud:

Electronic fraud is considered a form of fraud in general, however it has characteristics that distinguish it and make it a special nature due to its association with technologies general in the information is provided as follows:

- Objective characteristics related to the subject of the crime:

Where the crime of the electronic fraud is based on defrauding through the internet and forcing the victim to hand over the money to the accused using fraudulent and fraudulent methods that make him fall into the between them is mistake that makes him hand over his money .Which is what the network the traditional crime of fraud is based on, except that the difference is the method used that is through cybercrime is the use of a computer to carry out a crime and steal the money of others ⁽¹⁴⁾ .

Where large companies and tourism agencies have recently appeared promoting study aboard, as they offer offers conditions and significant sums of money, but unfortunately people are surprised by the existence of a fraud that is difficult to avoid claiming refunds or even pursuing the criminal.

- The term electronic fraud refers to any type of deception or scam that uses one or more internet services such as chat rooms, e –mail, internet forums, or web sites in order to send deceptive calls to potential victims on the internet with the aim of taking their money either by stealing credit card numbers, or send money orders or checks or be prompted to disclose personal information for the purpose of espionage, impersonation, or obtaining their account information in a sensitive center ⁽¹⁵⁾ .

The term electronic fraud appeared with the increase in the number of social media users on the one hand, and on the other hand, the increase and multiplicity of means of communication and media.

- Personal characteristics related to the person of the criminal:

Cybercrime in general and electronic fraud in particular are distinguished from traditional crime by committing the crime by a cyber-criminal with a high of intelligence and technical skills informatics ⁽¹⁶⁾ .

The crime of electronic fraud and defrauding people through the internet can be committed and executed easily, it does not need expert person or programs specialized in the field of the internet, but rather it can be implemented through social networking accounts, impersonation, and fraud via chat boxes.

Therefore, the definition of electronic fraud and the features that distinguish it can be derived as follows:

Electronic fraud is defined as a form of traditional fraud, which is the use of fraudulent methods stipulated by law by falsifying the truth, forcing the victim to hand over his money believing the truth in the order to achieve illegal financial profit, but what distinguishes it from traditional fraud is the use the internet is a means to carry out the criminal scheme and the criminal has the competence and knowledge to carry out the scheme what makes it a cybercriminal, and it is characterized by its

speed, ease of implementation, and difficulty in proving it .

2 – The need to change the traditional mechanisms of protection:

Given the specificity of electronic fraud, which is based on the presence of a spider web that is a fertile place for the commission of illegal acts, and given the alarming rise of electronic crime in general ⁽¹⁷⁾ and the crime of fraud in particular ⁽¹⁸⁾, it was necessary for the Algerian legislator to search for effective protection that guarantees protecting interests that are legally protected, such as protecting the right to property and ensuring the credibility of trust in transactions protection is represented in the search for preventive protection and repressive protection:

2 – 1 / Preventive protection:

Before addressing the preventive protection of electronic fraud the most important methods of fraud and swindling via the internet must be highlighted, which are:

- In the case of buying from famous websites, the person creates fake page for those websites in order to be able to attract people defraud them, and seize their money.
- Fraud and swindling can occur by hacking devices by sending a link, and then the individual clicks on it, and his personal data and information are withdrawn, and in most cases he is bargained over and forced to paying exorbitant amounts of money in exchange for retrieving his information or avoiding publishing on the internet when citizens carry out financial transfers, it is necessary to ensure that the data and information are correct “ so as not to let one of the fraudsters have a loophole through which they can defraud him.
- Recently, companies and tourism agencies have appeared that promote study abroad, as they offer huge offers in exchange for exorbitant sums of money, but unfortunately people are surprised by the existence of a fraud and swindling, after which it is difficult to claim recover these amounts or even pursue criminals.
- Recently charities have appeared that are active in solidarity work, but to take people's money and defraud them.

That is why it was necessary to look for protection of a preventive, nature represented in:

- Avoid entering any link of unknown origin when you receive it on a social media browser or through text messages that you receive on a mobile phone.
- Do not make your personal data public.
- Use privacy protection measures adopted by social networking sites to provide you with adequate protection.

- Do not impress by the tempting offers that appear to you through the social network or the internet its credibility verifying after.
- You must be careful and avoid communicating with people who do not have relationship.
- You must aware and report that you have been exposed to fraud by contacting the security services competent.
- Establishing information crime combating teams affiliated to the national security directorates and the national gendarmerie, as these departments confirm through their official pages on Facebook on twitter their awareness campaign about fraud and swindling crimes via the internet, and through which they call on parents to be vigilant against the tricks of professionals (hackers),and fraudsters who they resort to fake messages that enable them to obtain personal data and secret words related to their victims personal accounts, or even steal their personal identity .They also claim to monitor children will using the internet and constantly educate them about its disadvantages⁽¹⁹⁾.
- The establishment of the national Authority for the prevention and combating of crimes of information and communication technologies⁽²⁰⁾ pursuant to article 13 of law N° 09/ 04, specifying the rules for the prevention and combating of crimes of information and communication technologies, its mission is to activate and coordinate the prevention of crimes related to information and communication technologies and to assist the judicial authorities and the interests of the police in the investigations it conducts regarding information crime and the completion of judicial expertise.

2 - 2 / repressive protection:

the laws regulating the criminalization of electronic fraud and swindling have become useless on the basis of changing data and the emergence of the world wide web that has dominated the world with its complexities and advantages, how to access and work with it, and the immaterial nature that is one of the most important difficulties in combating it, for this, it was necessary to search for other ways to deter cybercrime in an efficient manner in general and fraud in particular :

- Criminalizing the act of fraud and swindling in the penal law⁽²¹⁾:

With reference to the Algerian penal law, we find that the Algerian legislator stipulated the criminalization of the act of fraud to denote fraud in its traditional sense in article 372 of penal law, whose material pillar is based on fraud which is an deception, that is distorting the truth regarding an incident that results in making a mistake, and this means that the essence of fraud is books and the subject matter of this lie⁽²²⁾ is an incident that results in creating confusion in the present's belief and

thinking and making him believe something other than the truth to the offender⁽²³⁾. However, this article is no longer feasible at the present time to be applied to the various fraud crimes that take place via the computer due to the specificity of this new crime, for which the internet is the fertile field for its commission. For this reason, the Algerian legislator amended the penal law in 2004⁽²⁴⁾ and included the seventh section bis in the articles from 394 bis to 394 bis 07 to criminalize any act committed via a computer under the title “affecting automated data processing systems”.

-Referring to the aforementioned articles, we find that the Algerian legislator has criminalized infringement of automated processing systems for data and classification of crimes into categories.

- Entering or remaining by fraud, in all or part of an automated data processing system (intentional assault on deleting or changing the system data or sabotaging the system's operating system data integrity within the system).

- Illegal dealing in data stored, processed or sent through an information system.

- It is noted through these articles that the Algerian legislator only criminalized acts that constitute an attack on the information system. It also tightened the penalties in amending the penal law of 2006 for the crimes listed in this section while keeping on the same crimes, because of its belief in the seriousness of this crime that took the direction of its spread and diversity, for this we can provide a definition of the crime of information systems as the intentional tampering with information and data representing a material value stored by the computer system or the unauthorized entry of correct information and data or tampering with commands and instructions that govern the programming process, or any other means that may effect the computer in order to obtain illegal profit and cause damage by other⁽²⁵⁾.

- But by going back and carefully looking at these article, we did not find that the Algerian legislator had singled out electronic fraud crimes in its articles, but rather it was limited to crimes related to automatic data processing, and given the existence of the principle of criminal legality, which stipulates that there is “no” crime no punished and no security measures without law. We can't the application of this text on the basis of the non-compliance of the committed incident with its legal form.

- The legislator also did not overlook the criminalized of electronic fraud if was committed through a network of criminal's, nor did he overlook the criminalization of participation, as article 394 bis 05 penal stipulates that “everyone who participates in a group or in an agreement formed for the purpose of preparing for one or more crimes stipulated in this

section .As for attempted crimes against automated data processing systems have the description of a misdemeanor, and according to the general rules, there is no punishment for the attempt to commit a misdemeanor unless the text is present, as article 394 bis 07 penal code stipulated that the attempt to commit misdemeanors stipulated in this section shall be punished with the penalties prescribed for the misdemeanor itself for the purpose of that a desire by the legislator to broaden the scope of punishment to include as many serious acts possible information systems ⁽²⁶⁾.

- And given that the Algerian legislator did not provide special texts to criminalize electronic fraud, we refer to the general rules for criminalizing fraud and in article 372 penal law on the basis of which we define the crime of electronic fraud as follows : “ seizing movable money owned by using fraudulent means stipulated in the text article 372 penal code, such as using false names or attributes, imaginary authority, financial dependence, or creating the hope of winning anything from it, and the computer is a tool in committing the crime meaning that the theft of others money is by using the internet”.

- The crime of fraud and swindle may also take other forms than those stipulated in article 372 penal code and one of its forms is what was stipulated in article 16 of law 18/05 ⁽²⁷⁾.

- No delivery of the contracted commodity despite the payment of its price as the electronic consumer has an obligation to pay the price in digital ways using a computer, but it is sometimes subject to fraud where he is unable to obtain what he contracted for despite paying the agreed price ⁽²⁸⁾.

- Promotion of a counterfeit product similar to an original product is expensive and of high quality.

- Promotion of an unknown good using misleading advertising ⁽²⁹⁾.

- **Criminalizing fraud in the law of preventing and combating crimes related to information and communication** ⁽³⁰⁾:

The Algerian legislator stipulated this law to complement the legal arsenal for confronting the problems related to information crime, and it included six chapters on the definition crime,, whose definition did not differ regarding what was stated in the penal code, and rules related to the inspection and control of the information system, also the establishment of the national authority for the prevention and combating of crimes related to information and communication technologies, and by referring to the provision of this law regulating the preventive and combative mechanisms of information technology crimes, we find the text of article 02 paragraph An information crime is defined as follows :

” crimes related to information and communication technologies mean all forms of crimes affecting automated processing systems, data specified in the penal law, and every crime committed or facilitated through an information system or electronic communication system.”

- It is noted on this article that the Algerian legislator expanded the article of criminalizing acts that fall within information crimes, as it is considered an information crime every act that harms the automatic data processing systems provided for in article 394 bis 07 of the penal law, as well as every act that is committed or facilitates its commission through an information system or electronic communication system.

- It is also noted that electronic fraud can be concluded in this type of crime, because it constitutes an act committed through an information system. The think that could lead to a violation of the principle of criminal legality stipulated in article 01 of the penal law, which states: “ there is no crime and no punishment, there are no security measures without the law”, meaning that the judge many not apply a crime not stipulated in the law .Nor is it permissible for him to decide a punishment other than those stipulated in the law ⁽³¹⁾.Which indicates that the penal code is the only source of criminalization and punishment, so the rest of the source, whether official or customary, that may be referred to in civil legislation, as excluded .One of the results of the principle of legality is that it is not permissible to interpret the texts extensively criminal law because the criminal law takes a narrow interpretation of its and rejects an a logy⁽³²⁾ .Therefore, giving the character of generality to the previous text can be understood as a violation of the principle of legality if we include other electronic crimes produced by successive technological developments, but the generality and lack of specificity expresses the flexible nature that legislation adopts in criminalizing, some acts that cannot be specified du the exploitation of criminals informatics of the increasing development in digital technology and its daily use in the commission of other crimes ⁽³³⁾.

- As for the extent to which the text comprehends all the forms of crimes related to information and communication technologies, it can be said that the text absorbed all crimes related to technology, but the legislator had to include a special text that would accommodates the crime of electronic fraud in the penal code in the section on criminalizing electronic crimes and considering it as one of the forms these crimes or stipulated explicitly in the special texts, because one of the characteristics of the criminal law is clarity and specificity, so that diligence is not carried out and a legal framework is established for it so that judges can follow up the perpetrators of the crime of electronic fraud ⁽³⁴⁾ .

- Establishing the national penal pole to combat crimes related to information and communication technologies:

Environment, in addition to given the technical nature of information crimes and their commission in a non- physical (digital) their wide in line with the widespread use of media and communication and the rapid development of its uses. The legislator prompted the intervention as usual in the year 2021 .Ad by amending the code of criminal procedure under order no 21 -11 ⁽³⁵⁾ and it has this modification included the creation of the penal pole, which specializes in combating informatics crimes which falls the states strategy against these types of crimes, as it represents an additional step in the path of combating information crimes.

- Algerian legislator like the French legislator, adopted the designation of crimes related to information and communication technologies in an attempt to extend the scope of criminalization to the maximum extent possible to include new crimes and in order to draw attention to the fact that criminal behavior goes by yond infringement or tampering with automated data to the use of the technological means to commit even crime in its traditional form ⁽³⁶⁾, contrary to the designations adopted by jurisprudence such as cybercrimes, information crimes, electronic crimes and internet crimes. Referring to article 211 bis 23 amending the criminal procedure law, we find that the legislator maintained the same definition of information crimes contained in article 02 /01 of law n ° 09- 04, related to technologies media and communication, but it was new in terms of :

- Determining the type of crimes that represent the exclusive, jurisdiction of the specialized criminal pole, as electronic fraud is considered among the criminal forms that complicate its jurisdiction before the pole.

- Using the term crimes related to crimes to information and communication technologies.

Conclusion:

After electronic fraud, one of the types of fraud in general, the demand for it has increased in the past few years due to the increase in social media users, as phishing crimes and fraud against individuals have increased in the diversity of areas of life, so the market, work and entertainment have become something that can be done easily while you are sitting at home or in the work office is on a network that can be described as a spider or via a mobile phone, with simple steps .It does not need experts or specialists in the field the internet .Rather, it can be implemented through social media accounts and impersonation .For this, electronic fraud is easier to implement than traditional fraud on the basis

that it is committed through a global communication network, which made the concept of fraud change with the change of its contents and data, and thus imposed the need to search for protective mechanisms that are in line with this change .

-Among the most important results that we have reached through this research paper are the following:

- Regarding the concept of electronic fraud:

Electronic fraud is defined as a form of traditional fraud, which is the use of legally prescribed fraudulent methods by falsifying the truth forcing the victim to hand over his money believing the truth in order to make an illegal material profit, but what distinguishes it from traditional fraud is the use of the internet as a means of implementing the criminal scheme, and that the criminal has the competence and know-throw to implement the scheme, which makes him a cybercriminal, characterized by the speed and ease of implementation and the difficulty of proving it.

-The concept of fraud has been linked to the meaning of fraud and they are considered two sides of the same coin, which is followed by Algerian legislation in considering fraud as an act using fraudulent methods that lead the victim to hand over his money to the perpetrator, as stipulated in article 372 of the penal law.

- Electronic fraud was associated with the general concept of information

Crime, which is based on the criminal's use of the internet to implement his criminal scheme, and access to the victims funds, as the criminal is characterized by information intelligence, acumen and technical skill that makes him a cybercriminal.

- Regarding the change of means of protection:

Due to the specificity of electronic fraud, which is based on the existence of a communication network that is a fertile place for committing illegal acts, it was necessary to change the means of protection against fraud, because traditional protection has become useless in the fight against technical fraud.

- Preventive protection:

It plays a very important role in fighting this phenomenon on the basis that prevention is better than cure, as the awareness role that individuals should play within the community is important in countering. Such actions, in addition to caution and awareness of the dangers of the internet.

- The establishment of the national commission for the prevention and combating of crimes of information and communication technologies under article 13 of the law 09/04.

- **Repressive protection:** it was represented in the mechanisms monitored by the state in order to combat electronic fraud, the most important of which are:

- The criminalization of fraud and swindling in the article 372 of the criminal law .However, this article currently no longer useful to apply to various computer fraud crimes due to the specify of this crime, for which the internet is the fertile field for committing .For this reason, the legislator amended the penal law in 2004 and included the seventh section bis in articles 394 bis 07 to criminalize any act committed by computer under the title of prejudice to automated data processing systems .However, after reviewing and screening these texts, we did not find that the Algerian legislator has singled out the crimes of electronic fraud with its texts, but was limited to crimes related to the automated processing of data, due to the existence of the principle of criminal legality, we cannot apply this provision on the basis of the non-applicability of the incident committed with its legal form. For this we can adopt the flexible criterion of the principle of legality, which benefits the inclusion of universality and generality in criminalization.

- He also expanded the circle of criminalization of acts that fall within the information crimes in the law on the prevention and combating of crimes related to information and communication technologies, N° 09/04, as every act that effects the automated data processing systems provided for in articles 394 bis to 394 07 of the penal law is considered an information crime, as well as every act committed or facilitated by an information system or an electronic communications system, which generally benefits in the inclusion of electronic fraud within this article.

- As for the extent to which the text accommodates all images of crimes related to information and communication technology, it can be said that the text accommodated all technology related crimes. However, the legislator should have included a provision that comprehends the crime of electronic fraud in the penal law in the section on criminalizing electronic crimes and considering it as a form of these crimes or explicitly stipulated in the special texts, because one of the features of the criminal law is clarity, specify and lack of diligence, so that judges can pursue the perpetrators of electronic fraud.

- The establishment of the national criminal pole to combat crimes related to information and communication technologies under the amendment of the code of criminal procedure in 2021, its task is to settle disputes committed in the digital environment, and electronic fraud is one of its forms and due to the absence of an explicit text confirming the legal description of the act of electronic fraud, which we can say that electronic

fraud is a form of traditional fraud, and therefore we can rely on traditional texts in determining the elements of the crime and its conditions and projecting all the data provided for the fraud introduced .

Bibliography:

1. Total dictionary of meanings, definition and meaning of fraud, consulted on 20/05/2022, hour 22.15, <http://www.almaany.com>.
2. Dictionary of Arab language, consulted on 20/05/2022, hour 22.15, <http://www.arabicdict.com>.
3. Agaohari bin Ismail Hammed, *The crown of language and Arabic Sahih The fifth part*, P363.
4. Ibn Mandour Mohammad ibn Bakr, *Arabic tongue, fifth part*, P 60.
5. John Larguier, *Criminal law of business, Library of Colin Armand, Fifth Edition*, Paris, PP 87,88.
6. Huda Kashkosh, *Computer scientist in comparative legislation, Arab renaissance House Cairo*, 1992, P20.
7. John Larguier, previous reference, P86.
8. Majhol Adab Satar, *Fraud crimes and the role of inspection offices in reducing them*, Baghdad, 2017, P02.
9. Hosni Mahmoud Naghib, *Summary in the explanation of the penal law, special section*, Arab renaissance House, Cairo, 1993, P 721.
10. Salah Shanin, *Criminal protection of electronic commerce, Doctoral thesis, Faculty of law, Tlemcen University*, 2013- 2014, P29.
- 11 – Law N°06 – 23, Publish it 20/ 12/ 2006, Amended and supplemented, included penal law.
12. There are those who adopted the term fraud including Tunisia, Lebanon, Jordan, Qatar, Oman, The united Arab Emirates, and Sudan, and there are some countries that adopted the term swindling such as Egypt,Marocco, Kuwait, and one the countries that used the term fraud is Somalia.
13. Shahira Bolahya, Douniazed Sayeh, *Electronic fraud, Journal of comparative and economic studies, The university center Si 2Alhawas, Barika, Batna, N° 2019*, December, P 39.
14. Monir Mohammed Al – Junaihi, *Internet and computer crimes and means of combating them*, University thought house, Alexandria, 2000, p135.
15. Types of internet fraud, *The free encyclopedia Wikipedia*, Consulted 05/ 06/2020, hour 22.00 pm, [www://ar-wikipedia.org/wik](http://ar-wikipedia.org/wik).
16. Saida Bouzagoon, *Combating cybercrime in Algerian legislation, Journal of the humanities sciences, faculty of law Constantine*, N° 50, 2019, P 48 .
17. Look .Nowara Bashoush, *Cybercrime terrifying numbers*, consulted on 25/05/2022, at 23.30 pm, <https://www.echoroukonline.com>.
18. As for electronic fraud, the police and gendarmerie recorded an amazing increase in the processing of electronic fraud cases, as the number of processed in 2020 reached 68 %within 152 fraud cases .Look, Said Abrkan, *152 cases of electronic fraud within 09 months*, consulted on 22/05/2022, at 23.30pm.
19. General directorate of national security consulted on 15/06/2022, at 18.00 pm, <https://www.algeriepolice.dz>.
20. Presidential decree N°15- 261, on 18/10/2015, defines the composition, organization and functioning of the national Authority for the prevention and combating of crime related to information and communication technologies, official journal N°35,issued in

08/10/2015.

21. Order N° 66/156, of the 08/06/1966, included penal law, Amended and supplemented.

22. Mahmoud Naguib Hosni, previous reference, P 723.

32. Abdul Erazzaq Al-Sanhori, *The mediator in explaining the civil law Part 01*, N° 162, P311.

24. Law N° 04/ 15, of the 10/11/2004, Amended and supplemented to order 66/ 156, Included penal law.

25. Samer Salman Abdul Jabouri, *Electronic fraud*, doctorate thesis, Nahrain University, Faculty of law, 2014, P 18.

26. Mourad Mashoush, *Information crime in the light of the penal law and the law of the prevention and combating of crimes related to information and communication technologies*, law journal, vol.09, issue 01, 2020, P120.

27. Law N °18/ 05 of the 10/05/2018 included electronic commerce, *Official journal*, N° 28, 16/ 05 / 2018.

28. Samia Alaib and Manal Araba, *Criminal protection of the consumer from the crime of electronic fraud*, *Herodotus journal of humanities and social sciences*, Vol.05, N° 03, 2021, P 232.

29. Same reference, P 233.

30. Law N° 09/04, of the 05 August 2009, Includes rules for the prevention and combating of crimes related to information and communication technologies, *Official journal*, N° 47, on 16/08/2009.

31. Abdoul Allah Solaiman, *Explanation of the Algerian penal law, General section, part 01, the crime*, Bureau of university publications, 2002, P 74.

32. Abdel Hamid El-shawarby, *Objective commentary on the penal law*, Maarif establishment, Alexandria, 2003, PP 18, 19.

33. Ilham Ben Khalifa, *The problems raised by paragraph A in article 02 from the law of the prevention and combating of crimes related to information and communication technologies*, *Journal of legal and political sciences*, The martyr Lakhdar Hama University, N° 10, 2015, P169.

34. The same reference, P 170.

35. The law N° 21/11 of the 25/ 08/ 2021, Includes the law of penal procedure, Amended and supplemented, *official journal*, N° 65.

36. Amina Ben Amiour and Ilham Bouhlaas, *National criminal pole for combating crimes related to information and communication technologies* *Journal of research in contracts and business law*, Vol.07, N° 01, 2022.