



CYBER FRAUD IN THE CONTEXT OF DIGITAL TRANSFORMATION - IMPLICATIONS AND SOLUTIONS

MAHMOUDI NOURELHOUDA¹.

¹Legal, Political and Religious Research Laboratory, University Abbès Laghrour Khenchela (Algeria).

The E-mail Author: mahmoudi.nourelhouda@univ-khenchela.dz

Received: 05/2024

Published: 11/2024

Abstract:

The crime of fraud has evolved significantly in the methods of unlawfully obtaining and misappropriating funds through various digital means and platforms, particularly social media. The fraudster uses digital communication tools to commit modern fraud, commonly referred to as cyber fraud. This crime is considered to be one of the most serious crimes, resulting in significant financial losses for the victims.

This study aims to make people aware of the dangers of this crime and to warn them against responding to these fraudulent messages. It emphasises the need to be vigilant and to check the credibility of the company they are dealing with before taking any action that could lead to financial loss. While this crime may be familiar to many in the context of digital transformation, its concept and implications for individuals and society remain largely unknown due to the lack of explicit legal texts at both local and international levels.

Keywords: Cyber fraud; Digital transformations; Implications and solutions.

INTRODUCTION:

Patterns of emerging crimes have multiplied and varied in response to the different spheres of life, with a significant focus on those crimes associated with the technological and digital revolution in general, and electronic crimes in particular. This has led to the emergence of behaviours that threaten digital security, a concept that has expanded to the point where it has become a serious concern in many countries, prompting governments to take measures to curb its spread in society. Among the most prominent of these emerging crimes is electronic fraud, a contemporary crime that threatens digital security and poses a real threat in our current era.

The phenomenon of e-fraud has grown with the advancement of technology and information, as well as the increase in the number of users of various social media platforms. This has contributed to the escalation and pervasiveness of the phenomenon, affecting both developed and developing countries, making it a global issue.


Whereas traditional fraud relied on the perpetrator using marketing or deceptive tactics to convince individuals or companies that they would receive something of value, today the digital realm has become a haven for them to acquire money effortlessly and without revealing the true identity of the fraudster. With the development of the Internet, electronic fraud has spread to numerous digital platforms, especially Twitter and Instagram, where social media sites of various kinds have become tools for luring individuals with the aim of seizing their money.

These crimes encompass various forms of fraud, including email scams targeting personal information, as well as tactics on Facebook and Twitter to lure individuals to suspicious sites and solicit financial assistance, promoting messages or advertisements claiming to offer business opportunities or prizes, with the ultimate goal of stealing personal information or money.

In order to combat these crimes, it is important to be aware of the potential methods used and to take preventative measures, such as avoiding providing personal information to untrustworthy sites and verifying the identity of senders before responding to such messages.

First: the importance of the research

Given the technological and informational advances brought about by various social media platforms, certain negative behaviours have emerged, facilitated by the use of these digital spaces. These platforms allow for the rapid dissemination of information with little effort, enabling individuals to



make financial gains by publishing messages containing requests and appeals related to fictitious investment operations. Fraudsters promise their victims high financial returns in exchange for their investments. The importance of the issue is therefore twofold:

Firstly, e-fraud is characterised by its transnational nature, crossing geographical borders and continents. Fraudsters can operate from anywhere in the world and target victims in different countries, making the fight against electronic fraud more difficult. This phenomenon has increasingly affected individuals and institutions, mainly due to the ability of fraudsters to operate behind screens, making it difficult to determine their true identity or location. This makes it more difficult to track them down and bring them to justice. Scammers often use a variety of techniques to obtain personal information such as credit card numbers and passwords, resulting in significant financial losses for individuals and businesses.

In addition, these activities contribute to undermining public confidence in legitimate and authorised institutions. People may be reluctant to engage with online services or even well-known organisations because of negative past experiences or a widespread fear of fraud. To rebuild this trust, the relevant authorities need to improve their security systems and educate the public on how to protect themselves from these risks.

The second aspect concerns the reasons for the proliferation of this phenomenon, which stem from a lack of deterrence and criminal accountability. It is therefore essential to update legislation with explicit provisions to prevent fraud in all its forms. Most victims of this type of crime find it difficult to prosecute and hold fraudsters accountable due to shortcomings in the legislation and legal loopholes in the criminal policy related to this crime. As a result, many fraud cases end in acquittals, case closures or decisions not to prosecute.

Aims of the research
This research aims to shed light on the contemporary electronic phenomenon of Internet fraud, which has proliferated due to legislative shortcomings in regulating this issue. It has become a negative phenomenon that fraudsters exploit for quick financial gains with minimal effort, requiring only basic knowledge of information technology.

In addition, this paper seeks to assess the effectiveness of current legal texts in curbing this phenomenon, which has evolved from its traditional form to a new manifestation using advanced technologies and means that have contributed to the alarming spread of this social plague. We will also examine the legal status of individuals who are victims of these crimes.

Previous studies

Research on this crime, particularly within Algerian legislation, has not been extensive. While there are numerous works and articles that address fraud from a traditional legal perspective, this study draws on various articles and publications that focus on cybercrime in general and fraud in particular. These include studies that examine the conceptual framework of this crime, as well as those that examine electronic fraud from a social or legal perspective. Among these studies, we note Dr Mohamed Hisham Saleh Abdul Fattah's legal research entitled "The Crime of Fraud", supervised by Dr Taha Nail, which discusses the elements of fraud and the penalties associated with it. This study addresses the challenge of distinguishing between fraud and related crimes that involve attacks on property and the legal nature of these crimes. However, our study focuses on the legal mechanisms to mitigate the dangers of electronic fraud within Algerian legislation.

In addition, there are several articles related to the crime of electronic fraud, such as Dr Boulehia Shahira's article entitled "Electronic Fraud", in which the researcher addresses the question of what constitutes electronic fraud in general.

Fourth: Research problem

The problem addressed in this study lies in the fact that electronic fraud is a relatively new phenomenon that has not been adequately addressed by criminal legislation. It is a complex issue facing the legal systems of many countries. Due to the dynamic and rapid nature of information

technology, most criminal jurisdictions have not updated their laws to reflect the emergence of this type of crime.

The problem raised by this study is the inability of judicial systems to prosecute these criminals, the lack of explicit legal texts dealing with this crime, and the failure of existing laws to keep pace with technology and the advent of the Internet, which has permeated various aspects of social, economic and political life. Electronic fraud is a new face of traditional fraud, and therefore the problem of the study stems from the act of fraud in general and electronic fraud in particular, in the light of the digital transformations, cultural openings and technological advances that the world is experiencing today.

These challenges have both positive and negative aspects: the positive ones include the use of digital platforms for beneficial purposes, while the negative ones relate to electronic fraud, which reveals legal violations, ethical contradictions and cultural conflicts. It is therefore essential to shed light on this phenomenon by addressing the following questions:

To what extent is current legislation sufficient to combat electronic fraud? Have existing legal texts become inadequate to prosecute electronic fraudsters and protect the victims of this type of crime?

V. Research Methodology

A descriptive and analytical approach was adopted to address this research problem. This method is necessary to describe the evolution of the crime from its simple, traditional form to its current manifestation, influenced by advances in science and information technology, known as electronic fraud. This type of fraud takes place in a virtual and immaterial environment, which makes it difficult to prove. The analytical aspect is particularly suitable for legal studies, which require an in-depth analysis of various legal texts related to the subject of the study.

In addition, a historical method has been used to understand the origins of this crime, which is both old and new, as well as the reasons for its recent proliferation, which has a direct impact on individuals and society.

VI. Research plan

The research is divided into three main sections:

1. Conceptual framework of electronic fraud: This section defines the key concepts related to the topic.
2. Implications of electronic fraud in digital spaces: This section examines the impact of electronic fraud on individuals and society.
3. Legal mechanisms to mitigate the risks of electronic fraud: This section discusses the legal frameworks available to effectively combat electronic fraud.

At the end of this research paper, we will conclude with a series of findings, recommendations and suggestions.

First: The conceptual framework of electronic fraud

The term “electronic fraud” has emerged alongside the early days of the Internet, and its rapid spread can be attributed to advances in the transmission and dissemination of information. These technological means have become accessible to almost all social classes, meaning that it is no longer limited to the rich or the poor, to a particular gender or age group. Furthermore, the ease of using the Internet, including the creation of accounts under fictitious names and assumed identities, has facilitated this phenomenon.

The low cost of such activities, requiring only a mobile phone or a computer connected to the Internet, has enabled fraudsters to engage in more fraudulent activities than ever before. As a result of the technological revolution in these various means, the methods of committing electronic fraud have evolved, allowing fraudsters to reach a larger number of victims. They are developing new techniques to steal financial and personal data, such as sending fake messages that appear to come

from trusted institutions to collect sensitive information, and using platforms to communicate with potential victims by presenting fraudulent offers to lure them in and gain their trust.

Definition of electronic fraud

Fraud is defined as deceit, trickery and cunning - any act intended to mislead contrary to its apparent nature. A person commits electronic fraud when they manipulate programmed information through improper programming, interfere with the execution of a program, use incorrect or incomplete data, or use any other method that results in damage to the property of others with the intent to unjustly enrich themselves or others¹.

In the following sections we will explore the concept of fraud as understood by sociologists and jurists².

1. Definition of fraud from a sociological perspective

Fraud, from a sociological point of view, is a social phenomenon that encompasses behaviours that contradict the prevailing moral values in society and have a significant impact on the private lives of individuals. It is seen as a practice that conflicts with human values. This implies that the social environment provides a fertile ground for such diverse practices³.

The roots of fraud can often be traced back to the social environment in which the fraudster grew up. The fraudster is first and foremost a victim of the social conditions that drive him to make money through fraudulent means. In this sense, fraud is a form of social dysfunction that may result from a decline in the fraudster's standard of living, although it is also true that many fraudsters may come from affluent backgrounds, which raises further questions.

The historical roots of electronic fraud date back to the early 1980s, specifically to 1981, when a new concept of computer crime emerged, associated with remote system intrusion and the activities of planting electronic viruses that destroy files and programs. This led to a characterisation of perpetrators of computer and Internet crimes, culminating in the term "electronic fraud"⁴.

In response to these developments, it became necessary to deal with these types of crime, in particular electronic fraud, which began to be recognised as a new category of crime. The first legislative response to these crimes was the Swedish Data Act of 1973, which addressed issues of computer fraud and included general provisions covering unauthorised access to, alteration of, or acquisition of computer data by various means. This was followed in 1978 by Florida's Computer Crimes Act, which criminalised computer fraud. In the early 1980s, many countries began to introduce similar legislation. Canada amended its Criminal Code to combat computer crime in 1983, and the US Computer Fraud and Abuse Act was enacted in 1984 and revised between 1986 and 1990. In the UK, Chapter 3 of the Computer Misuse Act 1994 criminalised electronic fraud⁵.

2. The definition of fraud from a criminal law perspective

Fraud, from the perspective of legal scholars, is not far from the definitions provided by sociologists. It is defined as any deception intended to mislead a person into making a mistake that leads him to surrender property in his possession. This results in the transfer of the property to the perpetrator or to another person, regardless of whether the deception is conveyed through speech, writing or gestures.

¹- Zamouche Ouidah and Yadjed Mohand Amziane, "The Phenomenon of Begging Between a Real Need and a Form of Work," Master's Thesis, Abderrahmane Mira University, Bejaia, 2014/2015, p. 08.

²- Moayad Hosni Al-Khawaldah and Abdullah Ahmed Al-Khesailat, "The Crime of Begging: A Comparative Study of Jordanian, French, Belgian, and German Laws," Turkish Online Journal of Qualitative Inquiry, Volume 12, Issue 3, July 2021, Research Article, p. 324.

³- Tahar Jalil Al-Habouch, "Fraud Crimes: Methods, Prevention, and Combat," Naif Arab University for Security Sciences, Research and Studies Center, Riyadh, 2001, p. 28.

⁴- Boulhia Chahira and Souih Dunya Zaid, "Electronic Fraud," Journal of Legal and Economic Studies, Si Al-Hawas University Center, Issue 04, December 2019, p. 42.

⁵- Boulhia Chahira, previous reference, p. 1339.

In criminal law, fraud is characterised as any statement of a past or present fact that the person making it knows to be false or is not convinced of its truth. Any intentional concealment or misrepresentation of the truth of a matter is considered fraud against individuals.

Electronic or informational fraud can be defined as a social plague that uses the virtual environment as a tool to perpetrate this type of crime. It requires a precise understanding of information technology and expertise in the use of deceptive methods, whereby the perpetrator misleads others by altering the truth or using tricks to gain unlawful advantage while causing harm to others.

It is important to note that e-fraud, like other crimes, has different factors that motivate individuals to commit it, making it different from other crimes such as theft, begging, bribery, etc. Despite the reluctance of most legal systems to prosecute perpetrators of electronic fraud, there are a number of reasons for this, the most important of which are the advances in information technology that fraudsters use to commit their crimes. The prevalence of such crimes varies from country to country, influenced by political, economic and social conditions.

Thus, electronic fraud is the act of illegally obtaining money from users and visitors of various digital platforms (such as Instagram, Twitter, Facebook, WhatsApp, email, etc.). This is done by exploiting these digital spaces without revealing the true identity of the fraudster and with minimal effort, as opposed to traditional fraud that takes place in public or private spaces. But what are digital platforms?

Definition of digital platforms (virtual environment)

Digital platforms are electronic programming platforms available on the Internet where individuals can open accounts, often under the names of virtual personas, while some may disclose their identities for personal interests. These platforms are used to exchange information and establish various relationships, whether for work, advertising, education or buying and selling, among others. One of the most striking characteristics of these platforms is their open and unlimited nature, which, due to their immateriality, has made the world resemble a small village, facilitating access to global events without the burden of travel or any material or moral effort.

It is important to distinguish between digital platforms and websites. The latter exist only on the Internet, while a platform is broader and more comprehensive than a website, as it combines two characteristics: the first is the provision of various interactive services, and the second, which it shares with websites, is the provision of information in various fields linked to public or private entities. A website, on the other hand, usually aims to provide specific information⁶ on a particular subject.

There are several types of digital platforms, including

1. Facebook

Facebook is one of the most widely used social media sites, allowing users to build numerous relationships and friendships. Its main feature is the ability to publish and upload various files, including studies, videos, pictures, applications and text messages. Facebook also includes many features such as chat rooms (Messenger), intelligent maps and the presentation of goods and services, making it a preferred platform for many users, including many fraudsters who create pages there⁷.

2. Twitter

⁶- Asma Nouri and Mohamed Aboud. "Digital Gateways and Platforms," Lecture Series on Traditional and Electronic Arabic References, Lecture 14, 2021, without publisher, pages unnumbered, available at: [Link] (accessed 22/10/2023 at 20:43).

⁷- Previous reference.

Twitter is a social media platform characterised by the posting of tweets. It serves as a tool that allows different software and systems to use content shared by many websites⁸. It allows users to keep up with the latest news from different sites without having to visit each site individually.

3. Instagram

Instagram is a mobile operating system that emerged alongside smartphones, with its application starting in 2007. One of its main features is the ability to share photos and videos through social media networks using hashtags. It also includes options for editing and applying effects to images using filters and dedicated tools⁹.

4. WhatsApp

WhatsApp is a free application that can be used without any financial cost. Due to its growing popularity, WhatsApp moved from a free to a paid service in December 2009. It is based on a centralised cross-platform messaging system for voice transmission over the Internet.

Section Two: The impact of electronic fraud on individuals and society

Electronic fraud is a crime that has no tangible physical effects that can be traced back to the scene of the crime. It takes place in the virtual digital environment, exploited by fraudsters through the exchange and dissemination of information via invisible digital waves. It also leaves no trace of the identity of its perpetrators.

One of the peculiarities of this type of crime is that it focuses on everything that is new in terms of information and technology, limiting its perpetrators to a specific group with a certain level of intelligence and digital knowledge. The nature of this crime differs from other crimes, such as theft of money or goods, in that victims willingly hand over their money to others. The e-fraudster uses deceptive methods, such as using false names or identities, or making false claims about specific incidents, to trick the victim into handing over their assets.

In addition, a single false call from a fraudster can result in thousands of victims, allowing for significant profits in a short period of time. This has encouraged many to engage in such behaviour, contributing to the rapid spread of electronic fraud compared to traditional fraud.

Electronic fraud is therefore an emerging crime and is considered to be one of the most difficult forms of cybercrime to detect and prove. Electronic crimes do not allow for witness testimony or interrogation, and they are transnational, which highlights the challenges and difficulties in detecting this phenomenon. Their existence is linked to advances in technology and information technology, which have recently led to the spread of these crimes in society, particularly in terms of the variety of platforms and websites used by fraudsters to commit these offences. A direct reason for this is the reluctance of most legislation and laws to prosecute the perpetrators of this crime, relying instead on provisions designed to combat traditional fraud.


In addition, this type of crime does not respect the geographical and local boundaries of countries in which it is committed. With the spread of the Internet across the world and different regions, many computers can now be connected to this network¹⁰, allowing scenarios where the perpetrator is in one country and the victim in another. Technological advances have effectively reduced distances and increased connectivity between different parts of the world, and this has an impact on the criminal nature of criminals who take advantage of these means to break the law. This means that the scene of electronic fraud is no longer local; it has become global, with the perpetrator not physically present at the scene of the crime, but committing the crime over the Internet and at a distance.

As a result of the legal nature of this crime, which is committed to satisfy individual needs and achieve financial gain and is primarily driven by greed and avarice, the prevalence of traditional

⁸- Mohamed Hisham Saleh Abdel Fattah, "The Crime of Fraud," Thesis Submitted to Fulfill the Requirements for a Master's Degree in Public Law, Graduate Studies Faculty, Nablus, Palestine, 2008, p. 52.

⁹- Asma Nouri and Mohamed Aboud, previous reference, pages unnumbered.

¹⁰- Hamada Khair Mahmoud, *op. cit.*, p. 270.



fraud has declined in comparison to electronic fraud. This is because cyber fraud requires a certain level of intelligence to perpetrate, unlike traditional fraud, which tends to focus on appearances and impersonation, misleading victims about the credibility of fictitious services and investments. As a result, many individuals have moved from traditional fraud to the newly emerging electronic fraud.

In addition, perpetrators of electronic fraud possess a high level of technical and informational knowledge, as well as an awareness of the latest developments in electronic tools and various types of social media. The diversity of these technologies enables them to commit their crimes with unparalleled precision and professionalism. Organised criminal groups involved in this type of crime are no longer confined to specific cities; they can now move freely and covertly across different platforms around the world. They can exchange information, plan operations and schedule specific times for execution by communicating via email platforms and social networks that are no longer confined to one country.

This situation complicates the search for forensic evidence that can be extracted from the virtual environment, which requires advanced information technology techniques. Such capabilities allow these criminals to quickly delete and manipulate data and information on computers¹¹. Consequently, the difficulty of detecting and proving these crimes has turned them into a profession practised by many individuals within society.

The lack of legal provisions to deter and prosecute these crimes, together with the lack of social regulatory mechanisms in many countries, contrasts sharply with traditional fraud, which has been addressed by most legal systems¹. These systems have defined the material, legal and moral elements of traditional fraud, explicitly outlining the prohibited acts and stating their illegality, together with appropriate penalties based on their severity. This is the approach taken by the Algerian legislator in the Penal Code

In this legal vacuum, the risks associated with electronic fraud have increased. The lack of clear and unambiguous legislation has contributed to the proliferation of this crime, allowing perpetrators to evade accountability and punishment. Even where laws exist to combat the crime, they often fail to address the evolving methods of electronic fraud and the advanced capabilities used in its commission¹². As a result, these provisions are not sufficient to fully mitigate the negative impact of this type of crime and to protect victims.

The continued increase in losses due to electronic fraud compared to traditional fraud, the growing number of people who are victims of these digital actions, and the resulting social impact have made it more urgent than ever to investigate this crime. This is because traditional fraud is easier to identify in terms of the perpetrators, the actions involved and the ability to gather evidence and witnesses. All of this leads to a quicker understanding of its dimensions and the apprehension of perpetrators at a lower cost. Electronic fraud, on the other hand, is not only difficult to detect and prove, but also very costly, both in terms of the planning involved in committing it and the losses incurred by the victims.

Section Three: Legal Mechanisms to Reduce the Risk of Electronic Fraud

The first step is to establish a comprehensive and effective overall strategy to mitigate the risks of electronic fraud. This is essential to ensure that efforts to reduce and monitor the phenomenon do not become merely reactive measures against such criminal activity without any real impact. Such a strategy should cover all aspects, whether at the national, Arab or even international level, in order to deal effectively with its negative consequences. No detail should be overlooked in order to avoid becoming an avenue for this crime or for any fraudster involved in electronic fraud.W

¹¹- Rania Atia, "Electronic Begging: Its Social and Economic Impact on Jordanian Society from the Perspective of a Sample of Facebook Users," *Journal of Humanities and Social Sciences*, Volume 5, Issue 4, March 30, 2021, p. 64.

¹²- Al-Kaabi Mohammed Ubaid, "Crimes Arising from the Unauthorized Use of the Internet," *Dar Al-Nahda Al-Arabiya*, Cairo, p. 34.

In particular, it is necessary for the legislative authority to create legal texts that address the issue of electronic fraud, which has become a phenomenon that threatens digital security worldwide. A review of various legislations, whether local, Arab or international, reveals a legislative gap, as most of their provisions only address actions and penalties related to traditional fraud. The latter has become completely different from fraud in its current form. This new type of fraud requires stricter penalties that are commensurate with this form of crime.

It is impossible to limit this crime to a specific pattern or to identify all the circumstances that have led to the adoption of such criminal behaviour. This directly contributes to the impunity of these electronic fraudsters. In addition, electronic fraud requires expertise and knowledge of the intricacies of electronic technologies, which means that investigators must approach it differently from other crimes. Investigators must also have adequate knowledge of information technology. Consequently, there is an urgent need to enact specific legislation for this type of crime, which would facilitate dealing with advances in digitalisation. Law enforcement agencies should improve their skills and modernise their methods to combat cyber crime. This includes providing appropriate training for judicial police personnel, using modern technology for data collection and analysis, and promoting international cooperation in combating cybercrime and sharing information between countries.

There should also be tougher penalties for cybercrime offenders, with changes and improvements to the legal framework to effectively combat these crimes and protect the electronic community. In addition, users must exercise caution and follow necessary security protocols when engaging online to reduce the incidence of fraud and various electronic violations.

The Algerian legislator addresses traditional fraud through Article 372 of the Penal Code¹³, which defines fraud as any act by which a person unlawfully obtains or receives money, valuables, securities, or any document, promise or receipt, or attempts to obtain any of these by deception with the aim of stealing all or part of another person's property. This may involve the use of false names, fictitious authority or misleading financial promises, with penalties ranging from a minimum of one year to a maximum of five years' imprisonment or a fine of between 500 and 20,000 Algerian dinars.

The Algerian legislator also considers the impersonation of roles, titles or names and their misuse as part of the crime of fraud. The purpose of fraud is not only financial gain; it can also be motivated by other motives, such as revenge, and can take various forms, as described in Articles 243 to 246 of the Penal Code.

However, it is evident that the legislator has not adapted to or addressed electronic fraud, which has become a source of income for many fraudsters in various forms. This omission indicates a lack of awareness of the impact of this phenomenon on individuals and society.

Despite the intervention of the Algerian legislator through Law No. 09/04 of 5 August 2009, which contains provisions to prevent and combat crimes related to information and communication technologies, it is noteworthy that this law does not contain explicit legal texts criminalising and penalising fraud committed through social media in general and electronic fraud in particular¹⁴.

The Egyptian legislator addressed the crime of fraud in Article 336 of the Penal Code, which prescribes imprisonment for anyone who unlawfully obtains money, goods, or financial documents by fraudulent means in order to seize all or part of another's property. This can be achieved by using deceptive methods that make people believe in a false project or fabricated event, create the illusion of a potential profit, or mislead them with false debts or forged documents. The definition includes acts involving the misappropriation of real or movable property that does not belong to the perpetrator or where the perpetrator lacks the authority to act. Thus, the Egyptian legislator, like the Algerian legislator, has addressed traditional fraud without specifically addressing electronic fraud.

¹³- Ababneh Mahmoud Ahmed, "Computer Crimes and Their International Dimensions," Dar Al-Thaqafa for Publishing and Distribution, Jordan, 2005, p. 16.

¹⁴- Law No. 66/156 dated June 1966 concerning the amended and supplemented Penal Code.

In contrast, legislation in developed countries has taken a different approach. For example, Sweden's Data Act of 1973 was the first legislative response to this crime, addressing computer-related fraud and including general provisions on unauthorised access to, falsification, alteration or unlawful acquisition of computer data¹⁵.

In addition, in 1978, Florida introduced a Computer Crimes Act in the United States, which criminalised computer fraud. In the early 1980s, many countries began to enact similar legislation. Canada amended its Criminal Code in 1983 to combat computer crime, while the United States enacted the Computer Fraud and Abuse Act in 1984, which was amended several times between 1986 and 1990. The United Kingdom also introduced the Computer Misuse Act in 1995, the third section of which specifically criminalises electronic fraud¹⁶.

At the international level, several agreements have been made on cybercrime in general, but no treaties or conventions specifically address the spread of electronic fraud. Despite the international nature of this transnational crime that crosses state borders, countries have not yet prioritised intervention through treaties or conventions to address this issue. Apart from a few conventions outlining procedures for investigating cybercrime, there is little in place to curb this phenomenon, which continues to escalate to the point where it is becoming increasingly difficult to distinguish between legitimate entities and those engaged in fraud¹⁷.

With regard to administrative and judicial mechanisms, these refer to the proceedings taken against these fraudsters. In cases where this type of crime is confirmed, it is essential to conduct thorough investigations into the circumstances and motivations that facilitated the commission of the crime. If proven, all necessary measures must be taken, in particular the confiscation of assets obtained through fraud, as well as tools and equipment used in the commission of the act, such as smartphones, software or computers, and the perpetrator should be referred to the competent judicial authorities.

CONCLUSION

Electronic fraud is a new type of crime that has emerged as a result of the digital revolution and the technological changes taking place in today's world. This environment has become a haven for many fraudsters who exploit individuals under false pretences to obtain confidential information or money through identity theft, document fraud or even threats. It is worth noting that the nature of this crime has affected all aspects of social and economic life and is reflected in various societies, both developed and developing. It has thus become an international and organised phenomenon. Through this research paper, we have reached a number of findings related to the spread of electronic fraud through digital platforms:

RESULTS:

1. Lack of legislation: There is a lack of legal texts criminalising this phenomenon and specifying the associated sanctions, which has led many to exploit this legislative gap at both national and international levels.
2. General legislative framework: The majority of legislation, whether Arab or international, and in particular the Algerian legislator, has remained vague and general, focusing on traditional concepts of fraud. This is despite the fact that many individuals have fallen victim to this type of crime, being deceived and robbed under the guise of reputable institutions presenting false investments, promises or waivers of obligations.
3. Characteristics of the crime: A notable feature of this crime is that it typically involves individuals who are well versed in information technology, which often allows them to hide the traces of their

¹⁵- Law No. 09/04 dated August 2009, concerning the special rules for the prevention and combating of crimes related to information and communication technology, Official Gazette No. 47.

¹⁶- Hamada Khair Mahmoud, *op. cit.*, p. 270.

¹⁷- Ubaid Ali, Nasser Mowafaq, et al., "The Nature of Cyber Fraud," *Journal of the Faculty of Law for Legal and Political Sciences, College of Law, Tikrit University, Baghdad*, [Link].

crimes. This complicates the situation of electronic fraud and many victims have not received justice from the competent judicial authorities in this digital context.

4. Challenges in prosecuting fraudsters: Due to the link between this crime and the technological means that have significantly contributed to the spread of the phenomenon, the pursuit and prosecution of these fraudsters remains unclear from an administrative or judicial point of view. Despite the enactment of numerous national and international laws on cybercrime, many perpetrators, particularly of electronic fraud, escape punishment and accountability.

SUGGESTIONS

1. Amend the legislation: The Algerian legislator should amend the provisions on fraud in the Penal Code to bring them in line with those of Western countries such as the United States and Sweden. Clear and specific texts on electronic fraud are needed, as the current provisions are no longer sufficient to keep pace with developments in this field.

2. Tougher penalties: Penalties for cybercrime, in particular electronic fraud, should be increased, given the recent alarming increase in this phenomenon, which is worrying in the absence of both general and specific deterrents.

3. Use of resources: All material and human resources should be devoted to the detection of electronic fraud in order to mitigate its negative consequences for individuals and society.

4. Monitoring and reporting: Continuous monitoring of the various actors in this field should be carried out under specific laws. Furthermore, it is crucial to promote a culture of reporting among citizens, especially in cases of fraud and scams on social media, as well as requests for help from individuals claiming to represent fictitious organisations and institutions. This is particularly important for those who are victims of such behaviour, which violates public order and decency in society.

REFERENCES

1. Legislation

- a. Law No. 66/156 of June 1966 on the Criminal Code, as amended and supplemented.
- b. Law No. 09/04 of August 2009, on specific rules for preventing and combating crimes related to information and communication technologies, Official Gazette No. 47.

2. Books

- a. Tahr Jaleel Al-Haboush, *Fraud Crimes: Methods, Prevention and Combating*, Naif Arab University for Security Sciences, Research and Studies Centre, Riyadh, 2001.
- b. Ababneh Mahmoud Ahmad, *Computer Crimes and Their International Dimensions*, Dar Al-Thaqafa for Publishing and Distribution, Jordan, 2005.
- c. Al-Kaabi Mohammed Obeid, **Crimes Resulting from the Unauthorised Use of the Internet*, Dar Al-Nahda Al-Arabiya, Cairo.
- d. Mohammed Hisham Saleh Abdel Fattah, *The Crime of Fraud*, Thesis submitted in fulfilment of the requirements for a Master's Degree in Public Law, Graduate Studies College, Nablus, Palestine.

3. Periodicals

- a. Boulehia Shahira, Swaeh Dunya Zad, "Electronic Fraud", *Journal of Legal and Economic Studies*, University Center Sih Al-Hawas, Breika, No. 04, December 2019.
- b. Obeid Ali, Nasser Mufaq, et al, "The Nature of Information Fraud," *Journal of the College of Law for Legal and Political Sciences*, College of Law, Tikrit University, Baghdad, www.iasj.net/iasj?func=fulltext&ald=124926.

4. Conferences

- a. Ahmed Asem Ahmed, "A Legal Perspective on Proving Defamation and Insult Crimes via the Internet in Egyptian Law", *First International Conference on Privacy and Information Security in Internet Law*, Cairo, 2008.

5. Web pages



- a. Asma Nouri and Mohammed Aboud, “Digital Portals and Platforms”, Lecture Series on Traditional and Electronic Arabic References, Lecture 14, 20-21, without publisher, available at [https://uomustansiriyah.edu.iq/media/lectures/8/8_2021_03_31!12_28_08_AM.pdf]. Date of acces :/22/10/2024 at 20:43

6. References in foreign languages

- a. Rania Atia, “Electronic Begging: Its Social and Economic Impact on Jordanian Society from the Perspective of a Sample of Facebook Users,” *Journal of Humanities and Social Sciences*, Volume 5, Issue 4, 30 March 2021.
- b. Hamada Khair Mahmoud, “The Crime of Electronic Begging and Ways to Confront It”, *International Journal of Advanced Research on Law and Governance*, Volume 4, Issue 2, 2022.
- c. Moayad Hosni Al-Khawaldah, Abdullah Ahmed Al-Khesailat, “The Crime of Begging: A Comparative Study of Jordanian, French, Belgian and German Laws”, *Turkish Online Journal of Qualitative Inquiry*, Volume 12, Issue 3, July 2021, Research Article.
- d. Zamouche Ouidah and Yadjed Mohand Amziane, “The Phenomenon of Begging: Between a Real Need and a Form of Work,” Master’s thesis, Abderrahmane Mira University, Bejaia, 2014/2015.