Journal of International Commercial Law and Technology
Print ISSN: 1901-8401

Website: https://www.jiclt.com/

Article

Electronic fraud affecting consumers in Algerian legislation

Article History:

Name of Author:
Dr. SAID Samira

Affiliation:
Mohamed Boudiaf University of M'Sila -Algeria.

Corresponding Author:
Dr. SAID Samira

How to cite this article:
Samira S, *et, al,* electronic fraud affecting consumers in Algerian legislation. *J Int Commer Law Technol*. 2026;7(1):461–467.

Received: *02-02-2025*
Revised: *08-09-2025*
Accepted: *01-11-2025*
Published: *04-02-2026*

Abstract: This study focuses on cyber fraud targeting consumers, a prominent form of economic crime in the digital environment, particularly in the Maghreb countries. Using Algerian legislation as a case study, we examine how perpetrators exploit e-commerce, online payment services, and fraudulent websites and applications to lure consumers into handing over money or banking information. These perpetrators employ sophisticated techniques that are difficult for the average consumer to detect. The study also highlights the fragmentation of the legal framework, encompassing the Penal Code, the Law on Combating Crimes Related to Information and Communication Technologies, the E-Commerce Law, and consumer protection laws. This fragmentation leads to challenges in the interpretation and application of legal texts. We identify the most common forms of consumer fraud (fake websites, phishing emails, fraudulent financial applications, and deceptive advertisements and investment schemes), emphasizing the elements of the material and moral elements of the crime, the harm caused, and the difficulties of proving the crime in the digital environment (evidence loss, multiple intermediaries, and the transnational nature of the crime). This study also addressed the limits of current protection, as well as the efforts of the judiciary and specialized bodies in addressing this phenomenon, before proposing a set of legislative, procedural and institutional reforms to enhance the protection of the electronic consumer from these crimes.

Keywords: Cyber fraud, online consumer, criminal protection, digital environment, electronic evidence.

INTRODUCTION

The rapid spread of e-commerce and online payment services in the Maghreb countries in general, and in Algeria in particular, has led to the emergence of cyber fraud as one of the most serious economic crimes in the digital environment. This is especially true given its direct impact on the consumer, who is considered the weakest link in electronic transactions. The importance of this topic is highlighted in the Algerian context by the increasing number of cases related to digital scams perpetrated through fake websites and pages, and the growing official awareness of the need to provide special criminal protection for the online consumer. Therefore, we pose the following question:

To what extent has the Algerian legislator, within the Maghreb system, provided effective criminal protection for the consumer against cyber fraud, in light of the rapid development of its digital methods and the diversification of its practical forms?

To answer this question, we have divided the topic into the following sections:

Section 1: Conceptual Foundations of Cyber Fraud

Section 2: Limits of Consumer Protection from Cyber Fraud and Means of Prevention

First Axis: Conceptual Foundations of Cyber Fraud

First - Definition of Cyber Fraud:

Most Arabic legal texts define cyber fraud as the use of technological or digital means (websites, applications, email, text messages, payment platforms, etc.) that include false or misleading data or offers with the intent of inducing the victim to hand over money or data that enables the perpetrator to seize their money or achieve an illicit economic benefit.(Al-Momani, Nahla Abdel Qader, 2008, p. 46.)

The Algerian legislator did not use a single,

explicit term for "electronic fraud" in its definition, but rather distributed the acts among traditional fraud, crimes of attacking automated data processing systems, and e-commerce crimes. This legislative choice leads the judge to rely on a dual classification: on the one hand, the elements of fraud, and on the other hand, the specificity of the electronic means as an aggravating circumstance or as an element of the material element.(Ali Abdul Qader Al-Qahwaji, 2004, p. 20.)

Second – The Legal Framework Governing Electronic Fraud in Algerian Legislation:

Criminal protection of consumers against electronic fraud in Algeria is based on a system of separate legal texts, most notably:

1- Provisions of the Penal Code relating to fraud and deception, and some texts specific to cybercrimes.

2- Law 09-03 relating to combating crimes related to information and communication technologies, which criminalizes attacks on automated data processing systems and the use of electronic media in committing financial crimes.

3- Law 18-05 relating to e-commerce, which adopts a protective philosophy for the online consumer by obligating suppliers to provide transparent and accurate data, and linking failure to do so to legal liability.

4- Various provisions in the Consumer Protection Law and the Postal and Electronic Communications Law relating to distance transactions and the advertising of goods and services. A study published in 2025 shows that this system, despite its relative comprehensiveness, suffers from clear fragmentation and the absence of a comprehensive legislative definition of cyber fraud targeting consumers. This affects legal certainty and the clarity of legal classification before the courts.

Thirdly - Elements of Cyber Fraud Against Consumers

Cyber fraud is a complex crime that requires the presence of a set of essential elements that constitute its legal structure. The perpetrator cannot be held accountable unless these elements are met, as stipulated by law. Like other crimes, it is based on two fundamental elements: the material element, represented by the criminal conduct committed by the perpetrator through the use of fraudulent means via electronic media; and the moral element, represented by the perpetrator's intent and criminal purpose, knowing that the act is illegal and criminalized by law, and that it aims to intentionally harm others. In other words, there must be a causal link between the criminal conduct, the intent and purpose to cause harm, and its actual occurrence.

1. The Material Element:

The material element consists of the perpetrator using a digital trick or deceptive technical means to entice the consumer into entering into a transaction or handing over money or data of financial value. Several practical forms of this have emerged in Algeria, the most important of which are:

- Creating fake websites or online stores offering goods at attractive prices, then collecting payment without delivering anything.

- Sending phishing emails falsely attributed to banks or telecommunications companies, requesting "data updates" or "payment confirmation," whereupon the victim reveals their bank card details, allowing the perpetrator to steal their funds.

- Developing fake financial applications that mimic the interfaces of electronic wallets or digital banks, used to collect login credentials or direct transfers to the perpetrator.

- Promoting, through sponsored ads and social media pages, fake investments or contests that request repeated transfers of small amounts or continuous payment information.

Legally speaking, any entry of false data or use of a misleading digital platform with the intent of making an illicit gain is considered an activity constituting the material element, whether the funds were seized directly or through two stages (collecting the data and then using it later). (Fatima Al-Zahra Ramdani, Ali Badrani, A, 2022, p. 866.)

2.The moral element

For the crime to be established, it requires the presence of general criminal intent, meaning the perpetrator's knowledge of the fraudulent nature of the means and its illegality in the digital environment, and his will to use it to deceive the consumer. It also requires specific intent, which is the intention to achieve illicit gain or to harm the consumer economically, whether by obtaining money directly or by acquiring data that enables him to do so at a later stage.(Osama Hamdan Al-Raqab, 2012, p. 53.)

3. The Element of Harm and Causation

Harm is often realized in the form of a direct financial loss, such as deducting amounts from the victim's account or depriving them of money paid for a non-existent good or service. Harm may also be indirect if their data is exploited to open accounts or conduct subsequent transactions that create obligations for them.

Causation raises practical issues in the digital environment, especially when there are multiple technical intermediaries or the actions of more than one actor overlap (website designer, marketer, recipient of funds). This necessitates that the judge rely on technical expertise to trace the path of data and transfers.

Thirdly - Practical Examples and Model Cases:

Academic research published in Algerian universities mentions a number of real-life examples that can be used in this study, with names and personal information changed to respect confidentiality:

- The case of a consumer who purchased smartphones from a website claiming to sell them at

low prices. He transferred the money via electronic transfer, and then the website disappeared without delivering the goods. In this case, the actions were classified as cyber fraud, with technical expertise being used to identify the owner of the domain and the associated bank accounts.

- A case involving text messages sent to several citizens, purporting to be from a well-known national bank, requesting "confirmation of a debit transaction" via a link. Some users entered their card details, resulting in successive withdrawals from their accounts. The legal proceedings were based on a combination of fraud, cybercrime, and forgery laws.
- Cases related to fake investment applications offering "trading" or "daily profits," where victims are lured with promises of high returns, only to have the application shut down after collecting substantial sums. These cases raised the issue of classifying the actions as fraud, unlicensed money transfers, and potentially money laundering.

These examples highlight two key points:

1- The evolution of fraud techniques from simple methods (primitive emails) to sophisticated platforms that mimic banks and financial markets.

2- The increasing reliance of the judiciary on technical expertise and cooperation with specialized cybercrime agencies to identify perpetrators and trace the flow of funds. Fourth – Challenges of Evidence and Procedure:

Studies indicate that proving cyber fraud presents particular difficulties, most notably the rapid deletion of digital evidence, the possibility of using external servers or digital identities, and the multiplicity of technical intermediaries between the victim and the perpetrator.

Among the practical challenges are:

- The Admissibility of Digital Evidence: The extent to which electronic records, log files, emails, and text messages are admissible as evidence, and the conditions for their validity in terms of the integrity of the source and the integrity of the chain of possession.
- The Speed of Data Protection: The importance of swift intervention by law enforcement to issue orders to data providers to protect data before it is lost or altered, a point the legislator has attempted to address in recent procedural amendments related to cyber economic crimes.
- International Cooperation: When platforms or domains hosted outside Algeria are used, the success of criminal prosecution depends on the effectiveness of international judicial assistance channels. This is a point of concern for all Maghreb countries due to the transnational nature of crime.

The establishment of specialized judicial centers for economic and digital crimes has led to a relative improvement in handling cyber fraud cases, in terms of accumulating expertise and developing working relationships with specialized security agencies. However, a significant number of cases are still closed due to the difficulty in identifying the perpetrator or their actual location.

Second Axis: Limits of Consumer Protection from Cyber Fraud and Means of Prevention

With the increasing prevalence of cybercrime and the growing reliance of individuals and institutions on digital media in their daily transactions, cyber fraud has emerged as one of the most serious threats to information security and undermines consumer trust in the digital environment. The real danger of these crimes lies in their sophisticated nature, relying on complex technical means and fraudulent methods that often outsmart traditional detection mechanisms. This necessitates an effective legal response and appropriate deterrents to protect individuals and maintain the cohesion of the economic and social fabric.

Therefore, focusing solely on punitive measures is no longer sufficient to combat this emerging scourge. It has become imperative to establish a comprehensive penal system that includes primary penalties commensurate with the severity of the offenses, and supplementary penalties that enhance deterrence and ensure justice. However, penalties alone remain insufficient to close the loopholes exploited by criminals. This necessitates the adoption of comprehensive preventative strategies that rely on modern technology and media and social awareness campaigns to cultivate digital literacy, thereby reducing the opportunities for these crimes and strengthening the resilience of individuals and institutions against them.

First - Penalties for Cyber Fraud and Deception Crimes

Cybercrimes, particularly fraud and deception, have become among the most prominent challenges facing legal systems in the digital age, given their severe material and moral consequences. This reality has necessitated decisive legislative intervention to establish deterrent penalties commensurate with the seriousness of these acts.

1- Primary Penalties

The crimes of fraud and electronic deception fall under the category of economic crimes that target the financial integrity of both individuals and institutions. The perpetrator deliberately deceives their victim, misleading them with false information or promises, in an attempt to gain illicit profits at their expense. Recognizing this danger, the Algerian legislator has given special attention to punishing these crimes through strict penalties aimed at achieving both general and specific deterrence. Below, we will review the most prominent primary penalties stipulated in the Algerian Penal Code.

- The penalties prescribed for the perpetrator of fraud or deception – if they are a natural person –

primarily consist of imprisonment and a fine. The Penal Code criminalizes these acts in Articles 372 to 379, specifying the penalties that can be imposed on the offender.

- Imprisonment penalty: Imprisonment is considered one of the most prominent criminal(Order No. 66-156, No. 30 of 2024.) penalties imposed on a natural person in fraud and deception crimes, where its duration usually ranges between one year and five years, depending on the circumstances of each case individually. It should be noted that this period is not fixed, but varies according to the seriousness of the act committed and the presence of aggravating or mitigating circumstances. (Article 372 of Order No. 66-156 containing the amended and supplemented Penal Code)

For example, if the crime was committed using forged documents, or if the victim is a vulnerable group such as the elderly or people with disabilities, the judge may lean towards a harsher sentence, imposing a prison term of up to five years. Conversely, the judge may reduce the sentence if it is found that the perpetrator committed the crime for the first time, showed genuine remorse, or sought to rectify the harm caused**.**

-Financial penalty: In addition to imprisonment, the perpetrator is subject to a financial penalty ranging from 100,000 to 500,000 Algerian dinars, at the judge's discretion, who takes into account several criteria, most notably the amount of money fraudulently obtained, the nature of the victim, and the complexity of the criminal scheme. This penalty may increase to one million dinars in certain cases, such as when the crime causes significant losses to a single victim, or when the harm affects a group of more than three people**.**(Article 372 of the same order).

The purpose of this fine is to achieve financial deterrence for the offender and to compensate for part of the material damage suffered by the victim, although the practical application of this penalty may face challenges, especially in cases of those who evade payment **.**(Ahsan Bousqia, 2023, p. 329.)**.**

- Penalties imposed on legal entities: Algerian jurisprudence and legislation have evolved to allow for the criminal prosecution of legal entities (such as companies and institutions) for crimes committed on their behalf or in their name by their representatives or employees, reflecting a modern trend in criminal policy.(Hussein bin Sheikh Ath Malouya, 2012, p. 237.) According to Article 18 bis of Law 04-15, a legal entity bears criminal liability if it is proven that the crime of fraud or deception was committed for its benefit and resulted from the actions or omissions of its organs or representatives. This includes crimes committed by employees or officials in the course of the organization's activities**.**(Mohammed Dweifi, 2009, pp. 251-263.)

If a legal entity is found liable, it will be fined five times the maximum fine imposed on a natural person. This means the fine could reach 2,500,000 Algerian dinars. This provision aims to hold institutions accountable for the conduct of their employees and to recognize them as partners in curbing illegal activities that could harm the national economy. In exceptional cases, the penalty may extend to the temporary closure of the institution or the imposition of restrictions on its activities as a preventative measure to ensure the crime is not repeated**.**(Farhawi Abdel Aziz, 2019, pp. 85-96.)

-Penalty for Criminal Conspiracy: Organized crime in the field of online fraud sometimes takes the form of "criminal conspiracy," a form of participation and premeditation that may be more serious than a single criminal act**.**

Criminal conspiracy, as defined in Article 394 bis 5 of the Penal Code, is coordination between two or more persons to commit a specific crime, even if this coordination does not reach the stage of actual execution. In fraud cases, this conspiracy may take the form of a network of fraudsters who distribute roles (website designer, identity thief, fundraiser, etc...

The law punishes mere participation in a criminal conspiracy with the penalty for the same crime that the conspiracy aimed to commit. If the conspiracy aimed to commit several crimes, the most severe penalty is applied. This legislative approach reflects the legislator's desire to dry up the sources of organized crime by punishing planning and preparation as well as execution. The Algerian legislator recognized the unique nature of cybercrimes and introduced amendments to the Code of Criminal Procedure to allow for more effective combating them. Given the transnational nature of cybercrimes, determining the competent court can be problematic. Article 37 of the Code of Criminal Procedure addressed this issue by permitting the transfer of the case or the conduct of the investigation to the location of the crime (the victim's place of residence) or any location where evidence of the crime is found, thus aligning with the nature of the digital space**.**

Through Articles 65 bis 3 and 65 bis 5 of the Code of Criminal Procedure, the legislator introduced modern investigative tools, authorizing judges to use interception techniques for electronic communications and recordings as a means of gathering evidence in economic and cybercrimes. This procedure is essential in crimes such as email or telephone fraud, where the evidence is purely digital and difficult to obtain through traditional methods. 2- Supplementary penalties**:**

In addition to the original penalties, the legislator realized the need for an arsenal of supplementary penalties that aim not only to punish the perpetrator, but also to dry up the sources of the crime itself, prevent the perpetrator from returning to it, and protect society from its long-term effects. These

penalties acquire exceptional importance in the field of cybercrimes, given their close connection to the technical means used in committing them.

- Supplementary Penalties in General Legislation:

A- Confiscation: Confiscation is considered one of the most prominent supplementary penalties. The law stipulates the confiscation of tools, devices, and software used in committing the crime or intended for this purpose. This penalty aims to disarm the perpetrator of their technological capabilities and prevent the reuse of these tools in subsequent criminal acts. However, the legislator has restricted this procedure to protect the rights of bona fide third parties. Therefore, funds or devices cannot be confiscated if it is proven that the true owner was unaware of their use in the criminal activity.

B- Closure of Websites or Premises Used in the Crime: The court has the right to order the closure of a website, technology center, or commercial establishment that was wholly or partially used in committing fraud or deception. This measure requires that the owner or manager of the premises be proven to have been aware of the criminal activity or to have actively sought to prevent it. This procedure helps to hold owners of digital platforms and internet cafes responsible for monitoring the activity taking place within their premises.

- Aggravating Circumstances: A crime may be accompanied by circumstances that increase its severity, leading to a harsher penalty. These circumstances include:

- Targeting of national or defense-related facilities.

- Committing the crime by a public official who abused their position.

- Deletion or destruction of the victim's digital data to conceal the crime.

In such cases, not only is the prison sentence or fine increased, but additional penalties may also be imposed, such as deprivation of civil rights or prohibition from practicing a specific profession or business activity for a defined period.

- Penalties under specific laws and competent authorities:

The legislator did not limit themselves to general law but also established supplementary punitive frameworks in relevant sectoral laws, and strengthened the role of specialized bodies in combating such crimes.

a- In the Postal and Electronic Communications Law: This law stipulates strict disciplinary penalties for employees in the telecommunications sector if they are involved in fraud or deception crimes that exploit the network or services of the institution. These penalties may include dismissal from employment, revocation of the professional license, or revocation of the institution's operating license itself, in an effort to ensure the integrity of a vital sector considered the backbone of the digital economy.

B- In the Insurance Law: The Insurance Law imposes administrative and disciplinary penalties on companies and intermediaries proven to be involved in or complicit in fraudulent activities that exploit clients' insurance data or electronic payment systems. These penalties range from fines and temporary suspension from work to criminal prosecution when necessary.

- The Role of Specialized Bodies:

Bodies such as the National Cybercrime Prevention Authority and the economic crimes units within the judicial system play a pivotal role in providing technical and judicial support. Their role extends beyond the technical analysis of digital evidence; they may also provide recommendations to the Public Prosecution or the court regarding preventative measures, such as blocking malicious websites, imposing technical monitoring on specific institutions, or temporarily disabling information systems until security vulnerabilities are addressed. This cooperation reflects the necessary integration between the legislative and executive branches in the fight against organized cybercrime.

Second - Preventive Measures Against Cyber Fraud and Deception

The massive expansion in technology use has made cyber fraud a daily threat to individuals and institutions. It has become clear that relying solely on penalties is like "closing the circle after the deed has been done." Therefore, there is an urgent need to build multi-layered preventive strategies that combine technical and administrative aspects on the one hand, and media and legislative aspects on the other.

1- Technical and Administrative Measures

Strengthening the digital security infrastructure and risk management within institutions constitutes the first line of defense against fraudsters. This effort branches into technical measures directed at the end user and administrative measures that regulate work within institutions.

A- Technical Measures for Consumer Protection: To ensure user confidence in electronic transactions, a set of security protocols and technologies has been developed:

- SSL/TLS and HTTPS Protocols: These are encryption technologies that guarantee the confidentiality and integrity of data transmitted between the user's device and the website, preventing eavesdropping or tampering. The appearance of a padlock icon in the address bar is a visual indicator of the use of this protection.

- Secure Payment Protocols (SET): Designed specifically to secure online financial transactions, these protocols integrate with bank cards and e-wallets, providing an additional layer of protection that ensures sensitive payment data is not exposed to intermediary websites.

- Electronic Encryption: A cornerstone of information security, it is divided into two types: Symmetric

encryption (such as the AES algorithm), which uses a single key for both encryption and decryption and is fast and efficient; and Asymmetric encryption (such as the RSA and ECC algorithms), which uses a pair of keys (public and private) and is the basis of digital signatures and secure key exchange.
- Electronic Signatures and Digital Certificates: An electronic signature is a unique digital "fingerprint" that proves the identity of the signatory and ensures that the document has not been altered since signing. Digital certificates are issued by trusted entities (certification authorities) to verify the public keys of individuals or organizations.
- Firewalls and Intrusion Detection Systems: These monitor data traffic to and from the network and block any suspicious activity, forming a crucial barrier against attacks. - Payment intermediary platforms (such as PayPal): These provide protection for both buyers and sellers by managing the payment process without directly exposing the merchant's bank card details.
B- Administrative measures within organizations:
The responsibility for building a digitally secure work environment lies with the senior management of any organization through:
- Establishing a clear information security policy: This is an official document that defines the responsibilities, standards, and security procedures that all employees must follow.
- Securing physical and logical access: This includes protecting data centers and server rooms from unauthorized access and managing access privileges to systems and information precisely (the "least necessary permissions" principle).
- Managing the employee lifecycle: This begins with security background checks upon hiring and ends with the revocation of all privileges and access upon termination, while encouraging periodic leave that may reveal ongoing manipulation.
- Creating a dedicated information security department or team: This team is responsible for continuous monitoring, responding to security incidents, updating systems, and raising employee awareness.
- Ongoing training and motivation: This involves conducting regular training courses on emerging security threats and linking promotions and incentives to adherence to security policies. - Regular backup and recovery strategies: Protecting data from loss due to attacks (such as ransomware) or failures.
Thirdly – Media and Legal Measures
In parallel with technical efforts, societal awareness and a sound legal framework play a crucial role in creating a digital environment hostile to crime. The challenge lies in building the trust of the online consumer, which requires specific legislation tailored to the unique nature of digital transactions. Algeria has taken steps in this direction through:
- Law 04-09 on Consumer Protection: which established general rules, although it needs further development to address the risks of the digital environment in detail.
- Law 04-18 on the Prevention and Combating of Cybercrime: which constituted an important step in criminalizing specific acts such as unauthorized access and attacks on information systems.
- The ongoing challenge: lies in the rapid evolution of fraud methods, which often precede the enactment of legal texts. This necessitates legislative flexibility and perhaps the adoption of broader and more comprehensive provisions, along with enhanced international judicial cooperation to prosecute transnational crimes. - Traditional and digital media are becoming vital platforms for building "community immunity" against fraud:
- Traditional media (television, radio, newspapers): These offer awareness programs and campaigns explaining common fraud methods (such as phishing and social engineering), disseminating official warnings from security and banking authorities, and discussing legal issues related to cybercrime.
- Digital media and social media platforms are used for the rapid spread of targeted information. Official bodies (central bank, police) publish tips and immediate warnings, organize campaigns using unified hashtags, and simplified awareness videos are shared on platforms like YouTube.
- Online journalism and specialized websites: These provide in-depth analysis of incidents, uncover new fraud methods, and offer practical guides for verifying websites and online merchants.
- Partnerships with the private sector and experts: Media outlets collaborate with cybersecurity companies and specialists to provide accurate technical content, contributing to raising the public's digital literacy.
- Educational content: Online applications and short quizzes teach users how to create strong passwords, activate multi-factor authentication, and identify phishing emails. Second – Mechanisms for Protecting the Online Consumer Against Fraud
A study published in 2025 concluded that the Algerian legislator has been "relatively better" at keeping pace with the evolution of criminal thinking by criminalizing online fraud, but has not yet achieved comprehensive protection for the online consumer due to textual fragmentation and some gaps in evidence and penalties.
The most important protection mechanisms are:
1- The preventive nature of the e-commerce law, which requires suppliers to provide clear and accurate information about their identity, the goods or services, their price, and the methods for canceling the contract, thus enabling consumers to distinguish between legitimate and fraudulent suppliers.
2- The criminal penalties prescribed for perpetrators of online fraud, which combine imprisonment and fines, with the possibility of additional penalties such

as prohibiting the accused from engaging in online business activities or confiscating the tools used in the crime.

3- Reporting and institutional protection mechanisms through cybercrime units within the security and gendarmerie services, and consumer protection associations that receive complaints and support victims.

Conclusion:

The analysis reveals that cyber fraud targeting consumers represents a complex form of economic crime in the Maghreb digital environment. It combines technological advancements with a lack of victim awareness and the challenges of cross-border proof. Despite legislative and institutional efforts, a number of reforms remain necessary, including:

- Adopting a unified and clear legal definition of cyber fraud in Maghreb laws, explicitly specifying its most common forms targeting consumers.
- Consolidating protective legislation for online consumers into a single legal framework or digital code to facilitate the application of relevant provisions by practitioners and judges.
- Supporting specialized training for judges and law enforcement officers in tracking digital transactions, analyzing electronic evidence, and dealing with cross-border platforms.
- Expanding partnerships between judicial authorities, regulatory bodies, banks, and telecommunications companies to detect early signs of fraud and establish shared databases on suspicious websites and applications.

REFERENCE

1. Al-Momani, Nahla Abdul Qader, Cybercrimes, 1st ed., Dar Al-Thaqafa, Amman, 2008, p. 46.
2. Ali Abdul Qader Al-Qahwaji, Criminal Protection of Electronically Processed Data, International Conference, 3rd ed., United Arab Emirates, 2004, p. 20.
3. Fatima Al-Zahra Ramdani, Ali Badrani, Legislative Shortcomings in the Field of Cybercrime in Moroccan and Algerian Legislation, Al-Ustad Al-Bahith Journal for Legal and Political Studies, Mohamed Boudiaf University of M'sila, Algeria, Vol. 7, No. 2, 2022, p. 866.
4. Osama Hamdan Al-Raqab, Fraud and Deception Crimes (Methods - Manifestations - Treatment), 1st ed., Dar Yafa Al-Ilmiya for Publishing and Distribution, Amman, 2012, p. 53.
5. Order No. 66-156 dated 18 Safar 1386 AH, corresponding to June 8, 1966, containing the Penal Code, Official Gazette, No. 49 of 1966, as amended and supplemented. By Law No. 24-06 of April 28, 2024, Official Gazette No. 30 of 2024.
6. Article 372 of Ordinance No. 66-156 containing the amended and supplemented Penal Code.
7. Ahcene Bousqia, A Concise Guide to Special Criminal Law (Crimes Against Persons, Crimes Against Property, and Some Special Crimes), Vol. 1, 24th ed., Dar Houma for Printing, Publishing, and Distribution, Algiers, 2023, p. 329.
8. Lahcen Ben Cheikh Ath Mellouya, Notes on Special Criminal Law, Crimes Against Persons and Crimes Against Property, Dar Houma for Printing, Publishing, and Distribution, Algiers, 2012, p. 237.
9. Mohamed Douifi, The Criminal Liability of Legal Entities in Algerian Legislation, Algerian Journal of Legal and Political Sciences, University of Algiers 1, No. 3, Vol. 46, 2009, pp. 251-263. Farhawi Abdelaziz, The Criminal Liability of the Legal Person in Algerian Legislation, Journal of Arts and Social Sciences, University of Setif 2, Volume 16, Issue 02, 2019, pp. 85-96