

Protecting The Electronic Consumer From Cyber Crimes

حماية المستهلك الإلكتروني من الجرائم الإلكترونية

Boukais Soumia*, Faculty of Law, University of Ain Temouchent

Soumia.boukais@univ-temouchent.edu.dz

Received: 06/04 /2026

Accepted: 20/05 /2026

Published: 31/05 /2026

Abstract:

This topic examines cybercrimes affecting the electronic consumer within the Algerian legal framework governing e-consumption. It begins by defining the electronic consumer and cybercrime, highlighting their key characteristics. The study then explores major forms of cybercrimes, including electronic fraud, misleading online advertising, and violations of legal obligations.

It also explains the legal basis and penalties provided under Law No. 18-05 on e-commerce and other relevant legislation. The findings show that the Algerian legislature has adopted both preventive and deterrent measures to protect electronic consumers by strengthening obligations and imposing sanctions. However, this protection still faces challenges, particularly in terms of enforcement and the difficulty of proof. Therefore, there is a need to enhance practical mechanisms and update the legal framework to keep pace with the rapid evolution of cybercrimes.

Key words: Protection- cybercrimes- electronic consumer-law.

Introduction:

Recently, the world has witnessed a significant development in the field of information and communication technology, which led to the prosperity of e-commerce and the widespread spread of digital transactions, and this transformation has led to the emergence of a new type of consumer, which is the electronic consumer, but the latter has become exposed to several risks in the digital space by falling victim to the so-called cybercrimes, which prompted the Algerian legislator to intervene in order to protect the electronic consumer through several legal texts.

Hence, the importance of this topic emerges as it deals with a modern and important issue in light of the rapid digital transformation, as it is necessary to protect the electronic consumer from the threats imposed on him by cybercrimes.

Therefore, this study aims to shed light on the phenomenon of cybercrimes affecting the electronic consumer, by analyzing the legal framework regulating e-commerce in Algerian legislation, and showing the effectiveness of legal texts in providing adequate protection to the consumer in the digital environment.

It also seeks to identify the various forms of crimes to which the electronic consumer may be exposed, with clarification of their elements and the penalties prescribed for them, and the main purpose of this study is to assess the adequacy and effectiveness of the legal protection prescribed for the electronic consumer.

In the face of this, we pose the following problem: **To what extent does Algerian legislation provide effective legal protection for the electronic consumer from cybercrimes?**

To answer this problem, we followed the analytical and descriptive approaches in our study, dividing the topic into two main axes, we will first deal with general concepts about e-commerce,

* Corresponding Author

the electronic consumer, and cybercrimes, and then we will move on to the legal and institutional mechanisms to protect the consumer from cybercrimes.

1- Conceptual Framework for the Electronic Consumer and Cybercrime

The digital environment has produced a special legal framework for consumer relations, which differs in nature from the traditional framework in terms of contracting, enforcement, and proof. This difference has led to the emergence of legal problems related to the determination of the status of the electronic consumer and the limits of protection set for it, especially in light of the imbalance between the parties to the electronic relationship

Accordingly, this topic aims to shed light on the conceptual and legal framework related to the electronic consumer, by defining its concept and stating its legal status, in preparation for studying the most important cybercrimes that affect him, and the legal mechanisms established to protect him.

1.1- Concept of the e-consumer

In order to clarify what is meant by an electronic consumer, it is necessary to first deal with the meaning of e-commerce, and then move on to explain what is related to the electronic consumer

1.1.1 Definition of E-commerce

There are many definitions of e-commerce according to each jurist, and this difference is due to the multiplicity of its application areas and the continuous development that accompanies it.

A. Jurisprudential Definition of E-Commerce

There are those who define it as a trade that takes place through the Internet or it is done through any medium such as the Internet or other electronic media¹.

On the other hand, there are those who define it as buying and selling processes that are supported by electronic means and based on the Internet, where electronic markets are in the field of the market instead of shopping places, where sellers use electronic marketplaces to present their products and services on an open line². Referring to the World Trade Organization, we find that it defined e-commerce as an integrated set of processes of concluding deals, establishing commercial links, and distributing, marketing and selling products through electronic means³.

The European Union has defined it as all activities that are carried out by electronic means, whether between commercial enterprises or consumers, or between each of them separately and between government departments, as well as the delivery of goods and services in a physical or moral form⁴.

B. Legal definition of e-commerce:

The Algerian legislator defined it through Article 6, paragraph 01 of Law 18/05 on electronic commerce⁵.

It is the activity whereby the electronic supplier proposes or guarantees the remote provision of goods and services to an electronic consumer through electronic communications. Although the definition presented by the legislator is broad and includes the stages of electronic commercial transaction, we note through it that it is flawed by a kind of shortcoming, as it did not elaborate on its definition of electronic commerce and did not specify the means adopted in trade such as the Internet, applications, and others, so it is preferable to expand this definition further.

By way of comparison, we find that the Tunisian legislator defined electronic commerce as commercial transactions carried out through electronic exchanges, and electronic exchanges as those carried out using electronic means⁶.

1.1.2 Definition of an electronic consumer

In it, we discuss the definition of the electronic consumer in jurisprudence and law:

A. Jurisprudential Definition

There is a narrow definition and a broad definition of the electronic consumer, with regard to the narrow definition, the electronic consumer is considered any person who contracts with the aim of meeting and satisfying his personal and family needs and desires⁷.

The French jurist Calais amoly defined it:

"A consumer is a natural person who obtains or uses goods or services for non-professional use."⁸

The broad trend defined it as any person who acts lawfully in order to use goods or services for the personal use of the supplier, and the supplier may be a natural person, company or producer, thus including commercial transactions between the producers themselves⁹.

It also means a person who purchases products or services from the electronic supplier and through the Internet, regardless of the means of payment used, as it is not required for the consumer to be considered electronically to use the electronic means of payment, the consumer may request a product or service and make payments in other ways¹⁰.

B. Legal definition of the electronic consumer

The Algerian legislature defines an electronic consumer through Article 06 of the Electronic Commerce Law, paragraph three, as any natural or legal person who acquires a good or service free of charge through electronic communications from the electronic supplier for the purpose of end-use.

Accordingly, through this definition, we find that the Algerian legislator excludes the person who purchases products in order to resell them, as here it is related to economic agents and not the consumer, only the consumer purchases the commodity for his personal purposes only and definitively, and thus the legislator has taken an important step in resolving the dispute over the concept of the electronic consumer, as he has precisely defined its definition and removed from its circle what is known as economic agents, since legal protection varies according to whether the person is a consumer or an economic aider.

1.2- Concept of Cybercrime

Cybercrime is considered one of the new crimes related to the field of information technology and technology, which makes it completely different from traditional crimes, whether through its content or through its characteristics as well, and in order to learn more about these crimes, it is necessary to address their various definitions and then their most important characteristics.

1.2.1 Definition of Cybercrime

It should be noted that there are several names that are called cybercrime, and there are those who call it cybercrime, and there are those who call it cybercrime or the crime of misuse of information and communication technology¹¹. It should also be called cybercrime or high-tech crimes, and it should be noted that this difference has also extended to the definition of cybercrime, as there is no comprehensive and agreed definition

of cybercrime, and on the basis of this, we will try to clarify the most important jurisprudential definitions first, and then we will address the legal definition of it.

A. Jurisprudential Definition of Cybercrime

Professor Merwie defined it as the illegal act in which the computer is involved¹².

There are those who define it as any positive or negative behavior whereby programs or information are attacked in order to benefit from it in any way¹³.

It is also defined as those crimes against property using information technology¹⁴.

There is a mixed definition that combines the means of committing it with its object, and it considers it to be a criminal activity that includes an attack on individuals or property committed using information systems through or located on computer equipment and networks, and which results in unlawful access to information or resources stored on the information systems for the

purpose of copying, canceling, transmitting, sabotaging, espionage or tampering with such information and data¹⁵.

b) The legal definition of cybercrime.

For the Algerian legislator, through Article 2 of Law 09-04, cybercrime has been defined as crimes of compromising the automated data processing systems specified in the Penal Code and any crime committed or facilitated by an information system or electronic communication system.

It should be noted that the legislature has called cybercrime the crime related to information and communication technology, and it is noted through the legal definition of the Algerian legislator that it has relied on two criteria, namely the criterion of the subject of the crime and the criterion of the means of committing it.

The Organisation for Economic Co-operation and Development (OCDE) has also defined it as any illegal, unethical or unauthorized conduct related to the automated processing or transfer of data¹⁶.

1.2.2. Characteristics of Cybercrime

A- Transnational crime

The Internet world does not recognize traditional borders and barriers between countries and continents, there are no checkpoints or transit centers in the digital environment, which has made this feature what distinguishes cybercrime due to the enormous speed of execution and the volume of funds and people targeted through it¹⁷.

Thus, when a cybercrime occurs, the perpetrator can be in one country and the victim in another country, and the damage may be in a third country¹⁸.

B- With an easy crime:

Committing an information crime does not require muscular effort, but depends on the mental abilities of the offender and the extent of his control over the computer and modern means of communication, he does not need to move or use a vehicle, and he may not even need anyone else to help him, as he can commit it while sipping a cup of coffee behind his desk¹⁹.

It is calm and comfortable, and there is no possibility that the perpetrator will be exposed to the risk of confrontation and resistance by the victim or by the security forces, as is the case with some traditional crimes.

In addition to the above, it does not require a large cost or huge funding to commit this crime, only the presence of a computer, an internet connection and some technology.

C. Difficult to prove:

This crime is characterized by its difficulty in proving and detecting it because it takes place in a digital environment different from the traditional one, where the elements of the crime are based in the computer and internet environment, which complicates the matter on the specialized investigative agencies²⁰, and it is also difficult to reveal the identity of the perpetrator, as the cybercriminal often uses means to hide his identity, which makes it very difficult to track him.

D. Soft crime:

It is a feature related to the difficulty of proof, as cybercrime is described as a soft crime, because it does not leave physical

traces like traditional crimes, as there are no breaks or blood stains, and what it leaves behind are digital traces that do not have a physical existence, and the means by which it is committed do not cause wounds or shed blood, but are electronic devices such as computers and technical programs with an attractive shape²¹.

In addition, there are other characteristics related to the cybercriminal, as he is characterized by the skill and experience to carry out his criminal act and may be a specialist in this field, as well as being a person who is not hostile, but who commits the crime often out of amusement, developing his skills, or obtaining money.

2- Legal and institutional protection mechanisms for the electronic consumer from cybercrime

The impact of digital development has not only changed the means of contracting, but has also extended to the nature of crimes affecting the electronic consumer, as they have become committed using modern technical methods that are difficult to detect and prove, and this reality has contributed to the complexity of the legal protection process, especially with the overlap of legal texts and the multiplicity of parties involved in combating them.

Accordingly, through this element, we will try to clarify the legal framework for the protection of the electronic consumer by studying the most important electronic crimes against the electronic consumer, and explaining their pillars and the legal penalties prescribed for them, in addition to the institutional role in addressing them

2.1- Legal protection of the electronic consumer from cybercrime

We will study this legal protection by reviewing the crimes that the electronic consumer may be exposed to, dividing them into

two types: traditional crimes committed in a digital environment and crimes created through electronic media.

2.1.1. Traditional crimes against the electronic consumer

These are those crimes committed against the electronic consumer, whether traditional or electronic commerce²².

A. The crime of deception

is doing some lies or some simple trick that would show that the object in question is contrary to the truth²³.

* **Legal adaptation:** Article 68 of Law 09-03 on Consumer Protection²⁴ and Article 429 of the Penal Code. Its Pillars: The Physical Element: Deceiving the consumer with false data about the nature, validity or source of the product. Moral Element: The intention to deceive the consumer and to know the existence of the penalty.

* **Punishment:** Article 68 of Law 09-03 on Consumer Protection and the Suppression of Fraud is referred to Article 429 of the Penal Code, and the offender is punished by imprisonment from two months to 3 years and a fine of 2,000 to 20,000 DZD, or by one of these two penalties. In case of aggravation (Article 430 of the Penal Code): up to 5 years imprisonment and a fine of 500,000 DZD. B. Commercial fraud crime:

Fraud is related to commerce in the e-society, and online commercial fraud is sold entirely within the scope of traditional commercial fraud, and also within the scope of cybercrime, as

well as it falls within the scope of economic²⁵ crimes. Legal adaptation: Article 431 of the Penal Code. Its Pillars: The Physical Element:

Creating counterfeit materials or goods

- Offering or placing counterfeit goods for sale
- Dealing in materials used in fraud and inciting their use
- Fraud issued by the administrator or accountant.

The means of the crime of fraud have been enumerated in Article 431 as exclusive, namely fraud in addition or confusion, fraud by diminishing, and fraud in industry²⁶.

* **Moral Pillar:**

The existence of the intention to cheating, i.e., the will of the perpetrator to investigate the criminal incident, knowing that the elements of the crime are available.

* **Punishment:** The legislator has stipulated penalties and other penalties in the form of violations that fall on the professional in the case of fraud in consumable materials and goods, fraud or possession of counterfeit goods, in Articles 288, 289, 429 to 435, where the legislator has stressed the obligations of the professional to protect the consumer: Referring to the text of Article 431 of the Penal Code, we find that the penalty for cheating is from two to 5 years imprisonment and a

fine from 10,000 DZD to 50,000 DZD. If health damage is caused: imprisonment from 5 to 10 years and a fine of up to 1,000,000 DZD. If it results in death: Imprisonment from 10 to 20 year

B. Fraud Crime

As for the crime of deceiving consumers through fraud and fraud, they are common in the field of electronic commerce as a result of the shady advertising of the characteristics of goods using fraudulent methods aimed at confusing the processes of analysis, quantity, weight, or quantity, or by fraudulently changing the composition, weight or volume of goods or products through false data²⁷. Legal adaptation: Article 430 of the Penal Code. Its Pillars: The Physical Element: The Use of a Means of deception.

Moral Element: The intention to seize the property of others.

***Penalty:** The penalty is imprisonment from one to five years, imprisonment from one to five years and a fine of 20,000 to 100,000 DZD. This penalty is applied even in the case of an incomplete offence, i.e. attempt.

2.1.2 New crimes committed through electronic media

Cybercrime Rapid technological development and increasing reliance on modern information systems and communication media in the field of commercial transactions have led to the emergence of a new type of cybercrime that directly affects the electronic consumer. Personal data, means of payment, and electronic signature have become vulnerable to attack through criminal acts committed remotely, without the need for the offender to be physically present at the scene of the crime.

In the face of the escalation of these crimes, the Algerian legislature hastened to strengthen the legal system with special penal provisions, whether by amending the Penal Code or by promulgating a law on electronic commerce, in order to provide effective penal protection for the electronic consumer. In this context, we will address the most important new crimes affecting the electronic consumer, for example, through the following:

First: The crime of unauthorized access to an electronic signature database

The connection between computers through information networks has facilitated the circulation of data and information on the one hand, and increased the risk of intrusion and illegal penetration on the other hand, as the information system has become vulnerable to penetration by people who are not authorized to enter or remain inside it.

The crime of unauthorized access to an electronic signature database is one of the most serious and widespread cybercrimes, which requires addressing its elements.

*** The material element**

The physical element of this crime is realized in every unauthorized entry or attempt to enter the information system, which is known as logical entry, and this is done by opening an outlet that leads to the automated data processing system, whether it is related to websites, computer systems, or communication networks.

The crime varies according to the forms of illegal entry, as it may be focused on the data itself, automated processing systems, or information networks.

*** The Moral Element**

The crime of unauthorized entry is considered a deliberate crime that requires the existence of criminal intent, which is to make the offender aware of the wrongfulness of his act and the direction of his will to commit it. The Algerian legislature does not require the existence of a special intention, since a general criminal intent based on knowledge and will is sufficient, in accordance with the text of article 394 bis of the Penal Code.

*** Punishment**

Article 394 bis of the Penal Code stipulates that anyone who enters or remains without a permit in an automated data processing system shall be punished with imprisonment from three months to one year and a fine of 50,000 to 100,000 DZD.

" Protecting The Electronic Consumer From Cyber Crimes "

The penalty is doubled if the act results in the deletion or alteration of the data, and is even more severe if the illegal entry or stay leads to the sabotage of the system's operating system, with the penalty of imprisonment from six months to two years and a fine from 50,000 to 150,000 DZD, with the attempt also criminalized.

Second: Prohibition of dealing through electronic communications in some goods and services

The Algerian legislature has defined a group of goods and services that are prohibited from being offered or sold through electronic means of communication, under Law No. 18-05 on electronic commerce, in order to protect the electronic consumer from risks that may threaten his health, security or public order.

***The material element**

The material element of this offence is achieved when offering or selling prohibited goods and services through electronic media,

which are defined in articles 03 and 05 of Law 18-05, and include: gambling, betting, lotteries, alcoholic beverages, tobacco, pharmaceutical products, products infringing on inviolable, industrial or commercial property rights, fireworks and firecrackers, and goods or services that require special legal formalities such as the sale of cars, in addition to sensitive equipment and products that affect national defense or public order²⁸.

***The Moral Element**

This crime is considered a deliberate crime, based on the general criminal intent, which is represented in the knowledge of the violator of the prohibition of the offer or sale of such goods or services, and yet he commits the act.

*** Punishment**

The legislature shall punish such violations with a fine ranging from 200,000 DZD to 1,000,000 DZD, with the possibility of shutting down the website for a period of one to six months, or deleting it from the Commercial Register, in accordance with Articles 37 and 38 of Law 18-05.

Third: Violation of the requirements related to commercial transactions and electronic advertising

The Algerian legislature has imposed on the electronic supplier a set of legal obligations related to the regulation of commercial transactions and electronic advertising, with the aim of ensuring transparency and protecting the electronic consumer from misinformation or fraud.

***The material element**

The material element is the violation of the obligations stipulated in Articles 11, 12, 25 and 30 to 34 of Law 18-05, such as the lack

of clarity of the commercial offer, the breach of the stages of concluding the electronic contract, the failure to respect the conditions of the electronic advertising, or the failure to keep the records of commercial transactions and send them to the National Center for Commercial Registration.

***The Moral Element**

This offence is considered intentional, and the criminal intent in it is achieved by the knowledge of the electronic supplier of the legal obligations imposed on it and the tendency of its will to violate them.

***Punishment**

In articles 39, 40 and 41 of Law 18-05, the legislature decided to impose fines ranging from 20,000 to 500,000 DZD, depending on the nature of the violation, with the possibility of suspending the activity of the electronic supplier or the suspension of electronic payment platforms, as well as taking additional measures such as seizing the means used in the commission of the violation²⁹.

In addition to all of the above, there are other crimes that we summarize as follows:

According to the Penal Code, the following acts are criminalized: - Modifying, deleting or falsifying electronic data. -Publishing or trading in digital data without permission.

- Forming an electronic villain association

As for the penalties stipulated, there are: Original penalties: imprisonment from 2 months to 3 years and fines of up to 500,000 DZD.

Supplementary Punishments: Site closure, confiscation, seizure of means, prohibition of activity. Attempted crime is punishable as a complete crime. Aggravating circumstances are if the crime affects public order or national defence. Law 20-05 on combating cybercrime, issued on April 28, 2020, includes the protection of personal data and provides for electronic censorship, searches, and seizures³⁰.

We find that although Algeria has a legal arsenal for the protection of the electronic consumer, it remains insufficient to cover all forms of complex cybercrime.

2.2- Institutional Protection of the Consumer from Cybercrime

The National Authority for the Prevention of Crimes Related to Information and Communication Technologies (NCT) is an administrative body of a special nature, established by Presidential Decree No. 19-172 of June 6, 2019, which establishes this body and defines its functions, organization and functioning³¹.

It was established as part of the national policy aimed at countering the growing cyber threats, including cybercrime affecting the electronic consumer, particularly those related to the infringement of personal data or the exploitation of information and communication technology for fraud and disinformation.

2.2.1. Legal nature of the Authority

Article 1 of Presidential Decree No. 19-172 states that the Authority is "an independent administrative authority of a special nature with legal personality and financial independence, and placed under the tutelage of the Minister in charge of communication."³²

Its core mission is to prevent cybercrime in all its forms, as well as to contribute to the preparation and implementation of the National Cybersecurity Strategy³³.

2.2.2 Organizational Structure of the Authority

The internal organization of the Authority consists of:

- The Chairman of the National Authority, who is primarily responsible for its management and representation before the authorities, judicial and administrative bodies.

- The General Secretariat is responsible for coordinating administrative work and implementing the decisions issued by the Chairman of the Authority.

Specialized technical committees, which are responsible for following up on technical developments, analyzing digital criminal activities and developing preventive plans³⁴³⁵.

- Studies and Analysis Unit, which prepares periodic reports on cybercrimes and makes recommendations.

- The Awareness and Training Unit is tasked with organizing awareness campaigns and media programs to raise the awareness of citizens and electronic consumers about the dangers of cybercrimes.³⁶

2.2.3. Functions and Functions

In accordance with article 7 of Presidential Decree 19.172, the Commission shall carry out the following functions:

- Study criminal phenomena associated with information and communication technologies and propose appropriate preventive measures³⁷.

- Coordinate work between the ministerial sectors and security and judicial institutions in the field of combating cybercrimes.

- Preparing awareness and training programs for citizens and professionals on information security³⁸.

- Cooperation with the competent international bodies to combat transnational cybercrime.

2.2.4. Its Role in Electronic Consumer Protection

- DEWA plays a pivotal role in protecting the electronic consumer from cyber risks through advanced preventive measures, as it works to:
- Monitoring threats to consumers' rights in the digital space;
- Supporting the capacity of law enforcement agencies to track cybercrimes;
- Coordinate with the National Authority for the Protection of Personal Data to ensure respect for the confidentiality of consumer data.

Conclusion:

At the conclusion of this study, it was found that the rapid development of information and communication technologies and the resulting expansion in the field of e-commerce have produced a new type of consumption, namely electronic consumption, which in turn has become exposed to increasing legal risks as a result of the spread of cybercrimes in its various forms.

The Algerian legislature has sought to address these challenges by establishing a legal system aimed at protecting the electronic consumer, whether through general laws such as the Penal Code, or special laws such as the Consumer Protection Law and the E-Commerce Law, in addition to laws related to combating cybercrimes.

Through an analysis of the legal texts, it is clear that Algerian legislation has recognized the electronic consumer and enshrined penal and civil protection for him, by criminalizing many acts that affect his rights, whether they are related to traditional crimes committed through electronic media, or new crimes related to information systems and digital data.

However, while important, these efforts remain insufficient to achieve effective and comprehensive protection of the electronic consumer, given the transnational nature of cybercrime, the sophisticated methods of committing it, the fragmentation and multiplicity of legal texts, the difficulty of proof in the digital field, and the limited technical training of some law enforcement agencies.

Based on the above, we make the following recommendations:

- The need to unify and regulate the provisions related to cybercrime in a comprehensive and integrated law that keeps pace with technological developments.
- Audit the legal concepts related to cybercrime and the electronic consumer to avoid ambiguity and interference in the application.
- Enhancing the technical training of judges and judicial officers to keep pace with crimes of a digital nature.
- Establishing specialized departments or courts in cybercrimes.
- Strengthening the role of the competent national authority and intensifying coordination between it and the rest of the security and judicial authorities.
- Developing international cooperation mechanisms to counter cross-border cybercrimes.

Thus, achieving real and effective protection of the electronic consumer requires a comprehensive legislative and institutional approach, combining punitive deterrence, prevention, and awareness, and adapting to the requirements of the digital age.

References:

-
- ¹ Akad, Y., The Legal System of Electronic Payment, Memorandum for Obtaining a Master's Degree in Law, Mouloud Maamri University, Tizi Ouzou, Algeria, 2011, p. 9
 - ² Amal Karam, K, E-Commerce, Bustan Al-Maarifa Publishing Library, Egypt, 2013, p.14
 - ³ Amina, A., E-Commerce, Political Encyclopedia, 2021, p. 2.
 - ⁴ Amina Omar, op. cit., p. 02.
 - ⁵ Law No. 18/05 of 10 May 2018 on e-commerce Official Gazette No. 28, issued on 16 May 2018.

⁶ Law No. 83 of 2000 on Electronic Exchanges and Commerce, promulgated on August 9 , 2000 , Article 2 , paragraphs 01 and 02.

⁷ The Electronic Sale of Counterfeit Goods through, GJardili-Shamal Al Internet, 01st Edition, Dar Al-Fikr Al-Jamia, Alexandria, Egypt, 2008,p. 66.

⁸ Calais auloy, J, temple, H, droit de la consommation d'alcool, 9ème, Paris, 2015 p78.

⁹ Abdullah Theeb, M., Consumer Protection in Electronic Contracting, 01st Edition, Dar Al-Farqa for Publishing and Distribution, Amman,2012, p. 38.

¹⁰ Lockley, N., Consumer Protection under the Algerian E-Commerce Law, 01st Edition , Khaldounia Publishing and Distribution, Algeria, 2024, p. 12

¹¹ SAdel Youssef , Cybercrime and the Crisis of Penal Legitimacy, Journal of the Kufa Studies Center, Faculty of Law, (7), Iraq, 2011,p. 112.

¹² merwe ,v, computer crimes an other crimes against information technology in South Africa. R.I.D.P. 2023 , p.54.

¹³ Amimer A., , Legal Challenges to Proving Cybercrime, University Publishing House, Algeria, 2024, p. .14

¹⁴ Khalifa Al-Malt, A., Cybercrimes, A Comparative Study, Dar Al-Fikr Al-Jamia, Alexandria, Egypt, 2005, p. 87

¹⁵ Suleiman, F, Cybercrime and its Impact on Financial and Banking Operations, Journal of Financial and Banking Studies(1),2015 , p. 7.

¹⁶ Organisation for Economic Cooperation for Development, (1986), Computer-Related Crimes, Legal Policy Analysis, UNCITRAL Library, Website.unov.tind.io.

¹⁷ Dweib, P., Arab Laws and Legislation to Criminalize Cybercrimes to Protect Society, Sixth Conference, Saudi Library and Information Association, 2010, p. 10.

¹⁸ Ganesh, A., Electronic Consumer Protection in the Light of Cybercrimes, International Journal of Legal and Political Transformations, 1(1),2022, p. 79.

¹⁹ Amimer, A., op. cit., p. 28.

²⁰ Al-Kaabi, A., Crimes Arising from the Illegal Use of the Internet, A Comparative Study, Dar Al-Nahda Al-Arabiya, Cairo, 2016 , p.04

²¹ Amimer, A., op. cit., pp. 28-29.

²² Bouzema, K., Criminal Protection of the Electronic Consumer from the Risks of E-Commerce in Algerian Legislation, Diaa Journal for Legal Studies, 03(02), 2021, p. 100

²³ Bourouh, M, Consumer Protection Guarantees under Law 09-03 on Consumer Protection and Suppression of Fraud, Memorandum for Obtaining a Master's Degree, Branch of Consumer Protection and Competition Law, Faculty of Law, University of Algiers, 2014/2015 , p. 16.

²⁴ Law No. 09-03 of February 8, on Consumer Protection and the Suppression of Fraud, G.R.O.C. 15, of February 8, 2009, as amended and supplemented.

²⁵ Bouhazma, K., op. cit. p. 102.

²⁶ Chetouh, R., Baaji, N., Consumer Protection from the Risks of Electronic Transactions - Preventive Aspects of the Electronic Contractor, Journal of Legal and Social Sciences, Ziane Achour University, Djelfa, (11) Algeria, 2018 , pp. 434-435.

²⁷ Mashrafi, A., Rafaf, L, Electronic Consumer Protection Mechanisms in Algerian Legislation, Journal of Legal and Economic Studies, 05 (1), 2022, p. 1958.

²⁸ Bouhazma.K., op. cit., p. 103

²⁹ Briwa. A, Boudiaf. A., Crimes Committed to the Electronic Consumer in Accordance with the Provisions of Law 18-05 Related to Electronic Commerce, Journal of Spaceal Ijtihad, Muhammad Khidir University, 12(2) Biskra,2020, p. 295

³⁰ Belmerdasi. R., Mechanisms for Protecting the Electronic Consumer from Cybercrime in Algerian Legislation, Comprehensive Journal of Law, Faculty of Law, University of Annaba, (1), 2022, pp. 78-80.

³¹ Presidential Decree No. 19-172 of 6 June 2019, Official Gazette of the Republic of Algeria, No. 37, issued on 9 June 2019, p. 37.

³² Presidential Decree No. 19-172, Article 1.

³³ Bouzbara. S., The National Authority for the Prevention of Crimes Related to Information and Communication Technologies: Between the Confidentiality of Electronic Personal Data and the Fight against Cybercrimes, Critical Journal of Law and Political Science, 17(2), Jijel University, 2022, p. 562.

³⁵ Buzbara. S., op. cit., p. 567.

³⁶ Buzbara. S., op. cit., p. 567.

³⁷ Presidential Decree No. 19-172, Article 7.

³⁸ Bouaoun, Z., The Role of the National Authority for the Prevention of Cybercrime in Consumer Protection, Journal of Humanities, (49) 01,2018 , p. .421