

## Legal Frameworks for Combating Cybercrime in Light of Algerian Legislation

الأطر القانونية لمكافحة الجريمة في الفضاء السيبراني على ضوء التشريع الجزائري

Hanane Medjahed<sup>\*1</sup>, Amina lagra<sup>2</sup>

<sup>1</sup> Media and communication studies laboratory ,University of Mostaganem, [hanane.medjahed@univ-mosta.dz](mailto:hanane.medjahed@univ-mosta.dz)

<sup>2</sup> Media and communication studies laboratory ,University of Bechar, [amina.lagra@univ-bechar.dz](mailto:amina.lagra@univ-bechar.dz)

Received: 01/03/2026

Accepted: 28./04/2026

Published:12/06/2026

### Abstract:

Cybercrime is considered one of the most significant emerging crimes, potentially causing far greater damage than traditional crimes. This has prompted many countries to expedite the development of legislative solutions to curb this phenomenon.

Cybercrime continues to spread rapidly due to the tremendous development in information and communication technologies worldwide. Therefore, this research paper used a descriptive-analytical approach to address the topic of cybercrime, its main characteristics, its most prominent forms and the legal mechanisms for combating it.

**Keywords:** Crime; Cybercrime; Cyberspace.

---

<sup>\*</sup> Author Corresponding

## 1. Introduction

Over the past two decades, the world has witnessed major and rapid technological transformations that have had many consequences, including the growth of cyber risks and threats, which pose a real challenge to the security of individuals and societies.

Cybercrimes are among the most dangerous crimes at present, especially with the increasing use of various digital technologies. Besides being distinguished by a set of characteristics compared to traditional crimes, cybercrimes today represent a new type of transnational crime, which has prompted the international community, including international and regional organizations, to take action and conclude numerous agreements. Agreements aimed at combating this type of crime include, for example, the Budapest Convention of November 2001. Existing institutions and laws were unable to eliminate or reduce it, which compelled states to reconsider their legislation and internal structures and develop a comprehensive legal framework. This is especially true given its evolving and rapid nature, and the need for a robust institutional structure with a high degree of technological control to effectively investigate and identify perpetrators. This necessitates a concerted effort to combat this phenomenon.

Algeria has not been immune to the repercussions of this new technological challenge, as evidenced by numerous security and scientific reports. This indicates a significant rise in the rate of these crimes, which affect the personal lives of citizens and also affect the security and stability of the country and all other aspects of life – economic, political, cultural, etc. Therefore, the Algerian legislator acted swiftly. To address the legislative gap by developing a specific strategy to confront these cyber threats and enacting a legal arsenal to combat cybercrime, based on the foregoing, we pose the following questions:

\*What is cybercrime?

\* What are the motives for committing cybercrime?

\*What are the types of cybercrimes and what are the appropriate means of protection and reduction?

To achieve the objectives of this research and answer its questions a descriptive-analytical approach was adopted to describe the nature of cybercrime and analyzing the specialized legal frameworks in Algerian legislation for combating it.

## **2. Concepts**

### **2.1 Crime**

Crime is defined as any behavior that violates societal norms and is punishable by law. It encompasses a variety of acts that range from petty theft to serious offenses such as murder. Crime is not only harmful to the individual victim but also has broader negative consequences for society as a whole ( Beshimov ,2024,p151).

Legal scholarship generally defines crime as "an unlawful act committed with criminal intent, for which the law prescribes punishment or a preventive measure." It is also defined as "any act criminalized by law, whether positive or negative, such as an omission, unless otherwise stipulated" ( Rouabeh, 2019,p29).

Crime is also legally defined as "the commission or omission of an act with criminal intent, harming a social interest protected by the legislator through rules that criminalize and punish it" (Al Jarallah, 2017,p 79).

### **2.2 Cybercrime**

The term cybercrime is used recently to refer to internet crimes that have emerged and developed as a phenomenon of crime related to information technology. These crimes

include any intentional act or omission related to the attack on physical or moral property or the violation of individuals' privacy.

The term cybercrime was coined by William Gibson in 1982, and since then the concept of cybercrime has expanded considerably. During its early years, scientists and institutions initially preferred to use the term computer crime in its narrow sense rather than cybercrime in its broader sense

As terminology evolved, academic efforts were made to define cybercrime as a comprehensive reference for a range of acts that target or utilize data or computer systems, in addition to other efforts encompassing crimes related to the violation of computer information or the exploitation of information resources for illegal purposes (Sebti & Bougrit, 2025, p205).

Others defined it as: "A criminal activity in which computer technology is used, directly or indirectly, as a means or end to carry out the intended criminal act" (Al-Qaraan, 2017, p19).

As for the Algerian legislator, we find that he did not settle on using a single term to refer to these crimes, as he called them "crimes affecting automated data processing systems" under Law No. 04/15 relating to the Penal Code. The term "crimes related to information and communication technologies" (Qadri, 2023, p324).

It was also used under Law No. 09/04 concerning the prevention of crimes related to information and communication technologies. These designations adopted by the Algerian legislator are considered indicative of cybercrimes. The Algerian legislator defined it under the provisions of Article 2, Paragraph A of Law 09-04 as: "Crimes against automated data processing systems as defined in the Penal Code, and any crime committed through an information system or an electronic communication system" (Law No. 09-04, 2009, p05).

According to the Algerian legislator, a cybercrime may be established as soon as the crime is committed, or facilitated through an information system or an electronic communication system, as the legal text clarified in the same context. The concept of information systems and electronic communications is addressed in paragraphs "B" and "C" of the same article. An information system is defined as "any separate system or a group of interconnected or related systems, one or more of which perform automated data processing to execute a specific program."

### 2.3 Cyberspace

Cyberspace is a virtual environment that relies in its infrastructure on modern technology in dealing and communicating between many actors, whether they are individuals, governmental, or non-governmental entities, through an electronic network (computer) that functions independently of traditional communication means, in other words, all the information and transactions circulating as much as they facilitate The process of integration between all communication devices and satellites, and cyberspace as much as it simultaneously creates vulnerabilities for hacking and unauthorized access"(Bouzdia,2019, p1265).

### 3.Characteristics of Cybercrime

Cybercrime differs from traditional crimes in the environment in which it is committed, as it requires the perpetrator to have technical tools to commit his illegal act and a minimum level of technical knowledge.

It is criminal behavior arising from committing an act prohibited by law or refraining from an act imposed by law. The characteristics of these crimes can be summarized in several points:

Technological medium: cybercrime is carried out using computers, networks, and the Internet as primary tools to commit illegal acts.

High level of secrecy: many cybercrimes are not reported, especially by institutions and commercial companies, due to fear of reputational damage or loss of customer trust.

Difficulty of detection it is difficult to detect because it leaves digital information traces rather than physical ones, making investigations more complex.

Transnational nature: cybercrimes often transcend national boundaries, potentially affecting multiple countries and causing widespread harm.

Technical expertise: perpetrators usually need advanced technical knowledge and experience in information technology and digital systems.

Non-physical nature: It is characterized by the absence of physical force and does not require the perpetrator to use corporal strength (Sebti & Bougrit2025,p205).

### **3.Forms of Cybercrime**

A. Cyber Attack on Computer Data: such as destroying data, information, and programs, and manipulating information stored inside the computer.

B. Cyber attack on the sanctity of private life:

C. \*It is by publicly disclosing private facts that affect a person, such as disclosing the fact that he is suffering from a shameful illness, is unable to pay his debts, or publishes a picture of his son.

D. \*Defaming a person in the eyes of the public.

E. \*Seizing certain personal items such as name, photo, and personal data related to private life. (Al-Zurfi, 2008,p38)

F. Blackmail and cyber threat: such as publishing true or false photos or information about the victim with the aim of obtaining money or an illicit relationship.

G. Cyber wiretapping: using software on the victim's device that allows them to view and listen to all conversations and correspondence coming from the victim.

H. Cyber attack on intellectual property rights: This occurs by attacking trademarks and patents, as well as copying, imitating, reproducing and manufacturing software without a license. It is an attack on financial and moral rights (Al-Shammari, 2016,p 52).

I. Seizure, Fraud and Cyber Fraud. Seizure, either for himself or for someone else, of movable property or a bond, or signing this bond, is through fraud, taking a false name, or impersonating an incorrect identity.

The Budapest Convention has divided crimes committed via the Internet into four major groups. The first group includes crimes that affect the privacy, integrity, and availability of systems and data, such as illegal access, illegal interception, data distortion, and system integrity. The second group includes crimes of forgery and fraud. The third group includes content-related crimes, such as the production and possession of pornographic materials using children. The fourth group includes crimes of assault on intellectual property and related rights.

#### **4. Types of Cybercrimes According to the Algerian Legislator**

##### **4.1 Crimes of Tampering with Automated Data Processing Systems**

These offenses are stipulated in Section Seven bis of chapter three felonies and misdemeanors against funds, of part two felonies and misdemeanors against Individuals, of book three: felonies and misdemeanors and their punishment of part two: criminalization,

amending and supplementing the algerian penal code No. 04-15 of november 10, 2004 it includes articles 394 bis to 394 bis 7 which are as follows:

- The crime of entering or remaining through fraud in all or part of the information system or anyone who attempts to do so, and according to the provisions of Article 394 bis in Law No. 04-15, "anyone who does so shall be punished by imprisonment from three (3) months to one (1) year and a fine from 50,000 DZD to 100,000 DZD." The penalty shall be doubled if this results in the deletion or change of the system's data. If the above-mentioned acts result in sabotage of the system's operating system, the penalty shall be imprisonment from six (6) months to two (2) years and a fine from 50,000 DZD to 150,000 DZD.

The legal text can interpret entry as fraud, for example, by deliberately hacking into systems and accounts, manipulating information, and exploiting it for certain purposes.

- The crime of fraudulently entering, removing or modifying data into an automated processing system, and in accordance with the provisions of Article 394 bis 1 of Law No. 04-15, "anyone who does so shall be punished by imprisonment from six (6) months to three (3) years and a fine from 500,000 DZD to 2,000,000 DZD".

- The crime of designing, searching, collecting, providing, publishing or trafficking in a deliberate manner and through fraud the data stored, processed or sent via the information system or possessing, disclosing, publishing or using for any purpose the data obtained from one of the crimes stipulated under the provisions of Article 394 bis 2 Law No. 04-15 Anyone who does so shall be punished by imprisonment from two (2) months to three (3) years and a fine from 1,000,000 DZD to 5,000,000 DZD.

\*The crime of participating in a group or agreement formed for the purpose of committing one or more of the crimes mentioned above. According to the provisions of Article 394 bis 5 of Law No. 04-15, anyone who does so shall be punished with the penalties prescribed for the same crime (Law no04-15,2004).

## **4.2 Crimes Related to Information and Communication Technologies**

The algerian legislator initiated new measures to confront electronic crime, including issuing Law 09-04. This law aims to establish special rules to prevent and combat crimes related to information and communication technology. It is the law regulating the information space in general and combating the criminal field related to it, by enacting rules that allow the prosecution of this type of crimes and their perpetrators

This law consists of six chapters that include a definition of cybercrime, provisions related to monitoring electronic communications, and procedural rules for inspecting information systems

In addition, a national authority for the prevention of crimes related to information and communication technology was established pursuant to this law. Its tasks include:

\*Activating judicial and security cooperation and managing and coordinating preventive operations Exchanging information with foreign parties in order to activate protection for the information system from every danger that threatens state institutions, national defense, or the strategic interests of the national economy (Law No. 09-04, 2009).

## **5. Subsequent Laws Supporting Law 09-04 to Reduce Cybercrimes**

### **5.1 Law No. 18-04 About the General Rules Related to Mail and Electronic Communications**

This law introduced and established a set of mechanisms to combat crimes related to cyberspace, including the creation of a regulatory authority whose tasks include ensuring that postal and electronic communications operators respect the legal and regulatory provisions related to postal and electronic communications and information security. ( Article 11 and 13 of Law 18-04 of May 10, 2018, which establishes the general rules

relating to mail and electronic communications, criminalize the violation of the confidentiality of correspondence sent by mail or electronic communications, or the disclosure of its content, publication or use without a license from the sender or addressee or news of its existence, criminalize the attempt to open, vandalize or transfer mail or assistance in committing this crime, Criminalizing the exploitation of electronic communications to harm the dignity and private life of others or to harm the lives of children, a set of punitive articles were enacted from 164 to 188 of this law ( Law No. 18-04, 2018).

## **5.2 Law No. 18-07 Related to the Protection of Natural Persons in the Processing of Personal Data**

The algerian legislator has established a set of mechanisms related to the protection of human dignity, private life, and public freedoms within the provisions stipulated in this law, including:

\*The establishment of a national authority to protect personal data. The purpose of personal data in this law is any information, regardless of its basis, related to a person identified or identifiable and referred to in this text as "the person concerned", directly or indirectly Especially by referring to the identification number or one or more elements related to his physical, physiological, genetic, biometric, psychological, economic, cultural or social identity.

\*The national authority shall take a set of administrative measures in the event of a violation of the provisions of this law.

The National Authority may conduct investigations and inspect the shops and locations where processing takes place, with the exception of residential shops.

\*Qualifying oversight agents to research and inspect crimes related to data of a personal nature under the supervision of the Public Prosecutor.

\*A plaintiff who infringes one of his rights stipulated in this law may request the judicial authority to take any precautionary measures to limit the infringement or to obtain compensation.

The algerian judicial authority is competent to prosecute these crimes committed outside the territory of the Republic by an Algerian, a foreign person residing in Algeria, or a legal entity subject to Algerian law ( Law No. 18-07 ,2018,p p 11-23).

### **5.3 Law No. 20-05 Related to the Prevention and Combating of Discrimination and Hate Speech**

The state has undertaken to develop a national strategy for the prevention of discrimination and hate speech in order to create public life and spread a culture of tolerance, dialogue and rejection of violence from society, by enacting a set of rules in this context in addition to establishing a national observatory for the prevention of discrimination and hate speech in speech, writing, drawing, signs, photography, singing, acting or any other form of expression, regardless of the medium used These crimes are committed at the level of the information system, as Article 30 of the law stipulates that anyone who commits these acts shall be punished with imprisonment from six months to three years and a fine from 60,000 DZD to 300,000 DZD. The penalty shall be increased in Article 31 to two years from 2 to five years and a fine from 200,000 DZD to 500,000 DZD if the crime is committed using information and communication technologies. The Algerian legislator also criminalized anyone who creates a website or electronic account dedicated to publishing information to promote any program, ideas, news, drawings or images that are likely to incite discrimination and hatred in society, with a prison sentence of 05 five years to 10 years and a fine of 5,000,000 DZD to 10,000,000 DZD ( Law No. 20-05 ,2020).

#### **5.4 Order No. 21-11 Established the National Penal Pole for Combating Cybercrime**

To complement legislative efforts in the field of combating crimes committed at the level of the information system, the Algerian legislator amended Book One of Order No. 66-155 issued in 1966 by adding Chapter Six

It is titled "National Pole for Combating Crimes Related to Information and Communication Technologies" and includes Articles 211 bis 22 to 211 bis 29.

A national criminal pole has been established to specialize in following up and investigating crimes related to information and communication technologies and crimes related to them, pursuant to the text of Article 211 bis 22 of the same law. The pole established across the national territory and exclusively is specialized in dealing with crimes related to specific information and communication technologies, exclusively, and crimes related to them, pursuant to the text of Article 211 bis 24, which limited these crimes to:

- Crimes that affect state security or national defense.
- Crimes of publishing and promoting false news among the public that could harm public security, peace, or the stability of society
- Crimes of publishing and promoting biased news that affects public order and security, of an organized or transnational nature.
- Crimes of trafficking in persons or human organs or smuggling of migrants.
- Crimes of discrimination and hate speech (Order No. 21-11 , 2021 , p 07-09).

#### **6. Conclusion:**

In conclusion to this research paper, we can say that cybercrime is a growing phenomenon that reflects contemporary challenges facing digital security, especially with the increasing reliance on the use of various digital technologies. These crimes range from

information theft and hacking to ethical issues such as blackmail, threats, and kidnapping by exploiting technical and psychological gaps in the digital system. They do not only affect the private life of the individual. Rather, it went beyond that to affect the safety, security and stability of countries, thus transcending the latter's national borders, which prompted the Algerian legislator to confront this criminal phenomenon by enacting and making amendments to the legal texts related to it to keep pace with its rapidly developing specificity, which changed the traditional view of crime. However, cybercrime remains more complex with the tremendous advances in information and communications technology, and is more difficult to prove and control except by technicians and experts in the field of automated systems. Cybercriminals are characterized by their ability to adapt to technological changes, which makes them difficult to hold accountable, in addition to their global nature that transcends geographical borders.

Ultimately, confronting this phenomenon requires enhancing public awareness, developing effective legal and technological tools, as well as strengthening international cooperation to maintain cyberspace security and protect communities from these growing threats.

## 7. Bibliography List :

1. Al Jarallah, A. B. G. A (2017) , *Internet crimes and their penalties according to the saudi anti cyber crimes law: a comparative study*, Dar Al-Kitab Al-Jami'i , Saudi Arabia.
2. Al-Qaraan, M. A (2017), *Electronic Crimes*(1st ed), Dar Wael for publishing and distribution , Jordon.
3. Al-Shammari, G. M (2016), *Cybercrimes* (1st ed), Dar Al- ilmiya dawlia, Jordon
4. Al-Zurfi, A. N. J (2008), *cybercrime affecting private life: a comparative study*, Al-Maktab Al-Jami'i Al-Hadith, Egypt.

5. Beshimov, B. I (2024), Philosophical definition and description of crime, *Irish Interdisciplinary Journal of science & research*, vol 8 no02.
6. Bouzdia, D (2019). Algerian strategy in the face of cybercrimes: challenges and future prospects , *Journal of legal and political sciences*, vol 10 no1.
7. Law No 04-15(2004),The Algerian Penal Code, *The Official journal of the Algerian republic*, no71.
8. Law No. 09-04(2009),On the prevention and fight against information and communication technology related crimes, *The Official journal of the Algerian republic*, no47.
9. Law No. 18-04 (2018), About the general rules related to mail and electronic communications ,*Official journal of the Algerian republic*, no27.
- 10.Law No. 18-07 (2018), Related to the protection of natural persons in the processing of personal data ,*The official journal of the Algerian republic*, no 34.
- 11.Law No. 20-05 (2020), Related to the prevention and combating of discrimination and hate speech, *The Official journal of the Algerian republic*, Issue 27.
- 12.Order No. 21-11 .( 2021), establishing the National Penal Pole specialized in combating cybercrime, *The Official Journal of the Algerian republic*. No 65.
- 13.Qadri, N. H. (2023). Cybercrime and mechanisms to combat it: facing cyber security challenges. *Algerian journal of law and political science*, vol 8 no 01.
- 14.Rouabeh, F (2019), Lectures on general criminal law, faculty of law and political science, Mohamed Lamine Debaghine Setif 02University.
- 15.Sebti , A & Bougrit, O (2025). Cyber crimes :its concept and mechanisms to combat it. *Journal of law and humanities Sciences* ,vol 18 no 01.