المجلة العربية لعلم الترجمة
Arabic Journal for Translation Studies
Vol: 5 / N°: 14 (2026)
ISSN: 2750-6142
OPEN ACCESS

# Cybercrimes and Mechanisms for Combating Them in Algerian Legislation

**Assia Zerrouki[1] & Rabie Maazouz[*2]**

[1]University of Ghardaia, Ghardaia, Algeria
[2]Ali Kafi University of Tindouf, Tindouf, Algeria

*Email 1: zerrouki.assia@univ-ghardaia.edu.dz*
[*]*Email 2 (Corresponding author): maazouz.rabie@yahoo.fr*
*ORCID iD 1 : 0009-0003-2264-0463*
*ORCID iD 2 : 0009-0004-9444-483X*

| Received | Accepted | Published online |
|---|---|---|
| 05/08/2025 | 19/12/2025 | 30/01/2026 |

: 10.63939/ajts.8tbhz362

**Cite this article as:** Zerrouki, A,. & Maazouz, R. (2026). Cybercrimes and Mechanisms for Combating Them in Algerian Legislation. *Arabic Journal for Translation Studies, 5*(14), 164-171. https://doi.org/10.63939/ajts.8tbhz362

## Abstract

With the proliferation and increase in cybercrimes faced by internet users in professional and personal transactions, and the increasing reliance on electronic data, it is necessary to develop a cybersecurity system at several levels. This information component has led to a change in the frequency and nature of cybercrimes committed.

The world has recently witnessed profound transformations at all economic, social, and cultural levels, particularly technologically. Societies have transformed from consumer societies to industrial societies to cyber-based societies, thanks to the rapid, low-cost, highly accurate, and highly profitable digital services provided by modern technology. Despite the positives of this technology, it has also posed a concern for every society, with its recognition of a number of negatives, the most important of which is what is known as cybercrime.

Given the specificity of these crimes—they transcend geography and do not discriminate between one society and another—Algeria is also among the countries that have witnessed a significant increase in the rate of these crimes in recent years. This has prompted Algerian legislators to enact legislation to combat cybercrime.

**Keywords:** Technological Developments, Cybercrimes, Digital Societies, Algerian Legislation, Crime & Internet

## Introduction

The world today is witnessing unprecedented development, especially in the technological field, which is closely associated with computing and computer systems. The world has increasingly become confined to a virtual space. This advancement has helped human beings by providing valuable services and ensuring greater comfort and convenience. People now manage their activities through electronic networks, particularly the Internet. However, despite its benefits, this development also brings negative aspects and risks that threaten individuals, companies, and even states, due to cybercriminal attacks on individuals' personal data, financial fraud targeting banking institutions, espionage, and cyberterrorism that has affected states in their public order and national security. Consequently, these states have become threatened in their very structure and existence.

Cybercrimes are among the most significant concerns that now trouble citizens in their personal lives and states in terms of sovereignty and security. This is because the enormous technological and digital progress—and its accompanying impacts at all levels—has greatly affected, or rather undermined, the security and stability of societies on the one hand, while the consequences of this technological revolution have come to infringe upon citizens' sanctity and privacy on the other.

In light of this new digital-technological challenge, states have sought to enact a set of legislation and to establish legal and institutional mechanisms to confront this type of crime, which has come to be referred to in academic literature as electronic crime or cybercrime.

Algeria is one of these states that has not been immune to the repercussions of this phenomenon. In recent times, crimes have spread that affect citizens' private lives and also threaten the country's security and stability, as well as other aspects of life—economically, politically, and culturally. They have even affected the social fabric in its structure and composition.

For this reason, the Algerian legislator has enacted several laws and regulations to combat cybercrimes. Among the most important is Law 09/04, which sets out the special rules for the prevention and suppression of offences related to information and communication technologies, along with other legislation aimed at limiting the spread of such crimes.

In light of the above, this paper seeks to raise the following central question: **To what extent are the mechanisms adopted by the Algerian legislator effective and efficient in combating cybercrimes?**

To address this issue, the paper will follow this plan:

- **Axis 1:** The concept of cybercrimes
- **Axis 2:** Mechanisms for combating cybercrime

## Axis One: The Concept of Cybercrime

Cybercrime has become a concept that is increasingly discussed in academic studies due to its importance in limiting cyber intrusions and confronting electronic crimes through various substantive and procedural methods. As a result, this term has come into wide use around the world.

### First: Definition of Cybercrime

The misuse of information and communication technologies by offenders is interchangeably referred to as Internet crime, computer misuse, computer-related crime, high-tech crime, and electronic crime. Electronic crime, as defined by the Association of Chief Police Officers, involves the use of a computer, the Internet, or technological networks to commit a crime or facilitate its commission. The Australian Institute of Criminology considers it a general designation for crimes committed through the use of electronic data storage or a communications device (Samir, 2017, p. 258).

Defining the meaning of Internet crimes is not an easy task, as it is a broad construct encompassing many types of emerging abuse and crime enabled by communication and information technologies. It includes harmful behaviors that occur in cyberspace, transcend geopolitical boundaries, and challenge law-enforcement investigative tactics and traditional methods (Badri, 2018, p. 134).

Cybercrimes pose a major challenge to the environment in which they are committed, as Internet offenders can operate from anywhere in the world and target large numbers of individuals or companies across international borders. The challenges increase due to the scope and scale of these crimes, the technical complexity of identifying perpetrators, and the need for international cooperation to bring them to justice. The Internet opens new opportunities for offenders based on the belief that law enforcement does not function in the online world (Ben Khalifa & Hafouza, 2017, p. 1).

### Second: Characteristics of Cybercrimes

The nature of cybercrimes and their distinction from traditional crimes is linked to the environment in which the crime is committed, as well as the tool or means used by the offender to carry out the unlawful act. Such crimes require the offender to possess knowledge—or at least a minimum level of technical literacy. They remain a form of criminal behavior that arises either by committing an act criminalized by law or by refraining from an act mandated by law. The offender's will is directed toward the act despite the existence of a legal text that criminalizes the conduct (Anini Sadiq, n.d., p. 37).

The characteristics of these crimes can be summarized as follows:

a) Crimes committed using a computer as a tool, with the Internet serving as the means (Hroual, p. 37).

b) Crimes that are often not reported, especially when they involve institutions and commercial companies, to avoid reputational harm or loss of customer trust (Mohammed, 2015, p. 65).

c) Crimes that are difficult to detect because they do not leave physical traces that can help solve the case; instead, they leave digital informational traces.

d) Crimes that are ambiguous and difficult to prove due to the absence of visible evidence, and because most data consist of symbols that cannot be readily read.

e) Transnational crimes that cause severe harm affecting multiple regions.
f) Crimes that require offenders to have technical knowledge and advanced expertise in computing.
g) Crimes that are generally non-violent, as perpetrators do not use physical force or bodily strength to commit them.

### Third: Types of Cybercrimes

Despite the diversity of acts that threaten cybersecurity, and the variation in their objectives and the actors behind them, some can be listed as follows:

1. **Violations of the confidentiality of communications** affecting access to email systems, chat services, file transfers, and access to information without authorization—similar to wiretapping phone calls, reading private email, or entering a home to search it. In countries that uphold legal rules, such acts generally require prior authorization from competent authorities in accordance with legal procedures. These acts—whether committed by an individual or by a public authority—violate rights and are considered crimes against rights.
2. **Manipulating, distorting, or destroying information** contained in certain systems—whether through physical intrusion or by sending software or specialized viruses—constitutes an infringement of property and the right to use and dispose of it. Where there is intent to cause harm, as well as interference with the proper functioning of a private or commercial website, whether the intended harm occurs or not, traditional crimes carried out via the Internet such as theft, fraud, deception, grooming minors, facilitating and encouraging illicit activities, and infringement of intellectual property rights are all punishable under positive law and do not require prior authorization from competent authorities in countries that adhere to legal rules.
3. **Crimes falling within the framework of organized crime**, such as money laundering and terrorism, which threaten the security of individuals and states in both cyberspace and the traditional sphere alike (Al-Ashqar, 2019, p. 220).

## Axis Two: Mechanisms for Combating Cybercrime

As a new step, the Algerian legislator enacted Law 09/04 on the prevention and suppression of offences related to information and communication technologies. However, the implementation of its provisions on the ground remains weak to this day, due to neglect of the technical aspects necessary for applying these provisions and for determining appropriate penalties against perpetrators. In many cases, sanctions are often limited to financial fines only (Atiya, p. 321).

### First: Preventive Measures

The Algerian legislator adopted a set of preventive measures to مواجهة cybercrime:

**1) Electronic surveillance**

This measure is permitted in specific cases, as exhaustively listed in Article 4 of Law 09-04 (Law 09-04 on the special rules for the prevention and suppression of offences related to information and communication technologies, 2009). It is carried out pursuant to a written authorization issued by the competent judicial authorities, for the prevention

of terrorist acts, subversive acts, or crimes affecting state security; or when information is available indicating a likely attack on an information system in a manner that threatens public order, national defense, state institutions, or the national economy. It may also be used for the purposes of ongoing judicial investigations and inquiries when it is difficult to reach results without resorting to this measure. Electronic surveillance may further be used within the framework of executing mutual international legal assistance.

**2) Cooperation with service providers to prevent cybercrimes**

This is achieved by requiring service providers to assist the authorities responsible for judicial investigations by collecting and recording, in real time, data related to the content of communications and by placing such data at the disposal of the authorities. This data includes:

- Data that makes it possible to identify service users.
- Data related to the terminal equipment used for communication.
- The technical characteristics, as well as the date, time, and duration of each connection.
- Data related to supplementary services requested or used and their providers.
- Data that makes it possible to identify the recipient of a communication, as well as the addresses of websites accessed.

Service providers are required to retain this data—referred to as traffic data. The law also defines it in Article 1 as "any data related to communication by means of an information system that is generated by the latter as part of the communications chain, indicating the source of the communication, its destination, the route taken, and the time, date, size, duration of the communication, and the type of service" (see Article 11 of Law 09-04).

## Second: Procedural Measures

Among the procedural measures adopted by the Algerian legislator are the following:

**1) Search and seizure of information systems**

For the purposes of protecting public order and meeting the requirements of ongoing judicial investigations and inquiries, a set of technical arrangements has been established to monitor electronic communications, collect and record their content in real time, and carry out search and seizure procedures within information systems (Meshoush, 2020, p. 15).

However, seizure procedures face several practical difficulties for technical reasons. This requires the authorities conducting the search to use appropriate techniques to prevent access to the data contained in the information system or to prevent copying of the data placed at the disposal of authorized users (Presidential Decree No. 20-183 on reorganizing the National Authority for the Prevention and Suppression of Offences Related to Information and Communication Technologies, 2020).

It is also worth noting that the law authorizes remote searches conducted swiftly on an information system or part of it, as well as the stored digital data within it. Remote searches may likewise be conducted on an information storage system. The competent authorities may requisition any person with technical expertise regarding the information

system under investigation, or the measures adopted to protect the data it contains, to assist them and provide any necessary information.

**2) Extension of jurisdiction over these crimes**

Jurisdiction is vested in Algerian courts to hear offences related to information and communication technologies committed outside the national territory when the crime is committed by a foreigner and targets Algerian state institutions, national defense, or the strategic interests of the national economy (Al-Ashqar, 2019, p. 240).

**3) Exchange of mutual international legal assistance**

The Algerian legislator allows for the exchange of mutual international legal assistance to collect evidence related to the crime in its electronic form. Requests for assistance aimed at exchanging information or adopting precautionary measures may be granted in accordance with international agreements and the principle of reciprocity (Meshoush, 2020, p. 18).

**4) The National Authority for the Prevention and Suppression of Offences Related to ICT**

This authority was established under Law 09/04. Its composition, organization, and operating modalities were left to be determined by regulation, and several amendments followed—starting with a presidential decree in 2015, then in 2019, until the 2020 presidential decree reorganized the authority and defined it as "an independent administrative authority with legal personality and financial autonomy, under the authority of the President of the Republic, with its headquarters in Algiers" (Atiya, p. 330).

Its headquarters may be transferred to any other location within the national territory by presidential decree. The authority consists of a Steering Council and a Directorate-General, both placed under the direct authority of the President of the Republic, and it presents reports on its activities (Hroual, p. 40).

**Based on the above, it can be observed that the Algerian legislator has taken a positive step by enacting and organizing this law; however, it is not sufficient on its own to address the seriousness of cybercrimes, which requires continuous adaptation to ongoing technological developments.**

## Conclusion

In light of what has been presented in this research paper, it has become an urgent necessity for both states and individuals to pay close attention to cybersecurity—especially as we live in the era of artificial intelligence. There is no alternative to cybersecurity in confronting cyber challenges and electronic crime. Algeria, through its criminal policy, has adopted a dual approach to addressing cybercrime, relying both on general traditional legal provisions and on special texts tailored to different fields. Despite the efforts made, Algeria still remains far from establishing a comprehensive criminal policy to confront this phenomenon. This is due to several obstacles that hinder the fight against cybercrime, particularly when newly introduced measures come into tension with the Code of Criminal Procedure and the requirement to respect human rights. Another challenge is Algeria's non-accession to international conventions in this field, especially the 2001 Budapest Convention on Cybercrime.

Accordingly, the following recommendations can be proposed:

1. The Algerian legislator should address deficiencies in laws related to cybercrime and accelerate the enactment of legal provisions concerning electronic forgery, especially since the 2010 Arab Convention on Combating Information Technology Offences addressed this issue, and Algeria has ratified it.
2. Establish a legal committee to draft legislative texts that align with and respond to developments in cybercrime.
3. Encourage international action to strengthen global cooperation and mutual legal assistance in combating cybercrime, particularly with advanced countries that have expertise in this field.
4. Promote a cyber culture among members of society and economic and financial institutions, and encourage the proper use of information and communication technologies.
5. Call on universities and institutes to organize events and conferences to raise awareness of the importance of cybersecurity and to curb cybercrimes.

## Disclosure statement

No potential conflict of interest was reported by the authors.

## References

- Official Gazette of the People's Democratic Republic of Algeria. (2009). *Law No. 09-04 of 5 August 2009 on the special rules for the prevention and suppression of offences related to information and communication technologies*. *Official Gazette of the People's Democratic Republic of Algeria*, (47), 16 August 2009.
- Official Gazette of the People's Democratic Republic of Algeria. (2020). *Presidential Decree No. 20-183 of 13 July 2020 reorganizing the National Authority for the Prevention and Suppression of Offences Related to Information and Communication Technologies*. *Official Gazette of the People's Democratic Republic of Algeria*, (40), 18 July 2020.
- Benkhalifa, A., & Hafouza, A. A. Q. (2017). *Cybercrime and mechanisms for combating it*. *Al-Imtiaz Journal for Economics and Management Research*, *1*(1), 148-170.
- Anini Sadiq, A. T. (2015). *Electronic crimes: Mobile phone crimes*. National Center for Legal Publications.
- Atiya, I. (2019). The status of cybersecurity within Algeria's national security system. *Misdaqiyaa Journal*, *1*(1). Faculty of Law and Political Science, University of Tebessa, Algeria.
- Bara, S. (2017). *Cybersecurity in Algeria: Policies and institutions*. *Algerian Journal of Human Security*, *2*(2), 255–280.
- Badri, F. (2018). Combating information crime in international and domestic law (Doctoral dissertation, University of Algiers 1 "Benyoucef Benkhedda", Faculty of Law, Algeria).
- Al-Ashqar, J. M. (2019). *Cybercrime of the era* (Vol. 1). Arab Center for Legal and Judicial

Research.

- Mukhtar, M. (2015, January). *Can states avoid the risks of cyberattacks?* (Cyber Security). *Trending Events*, (6), 5-6. Future Center for Advanced Research and Studies, Abu Dhabi, United Arab Emirates.
- Meshoush, M. (2020). *Information crimes under the Penal Code and the law on the prevention of offences related to information and communication technologies*. *Al-Qanoun*, *9*(1), 109-133.
- Heroual, H. N. (2014). *Internet crimes: A comparative study* (Doctoral dissertation, Faculty of Law and Political Science, Abou Bekr Belkaid University of Tlemcen, Algeria).