

Legal Mechanisms for Combating Cybercrime in the Era of Artificial Intelligence

**Responsible Authority: State Property
Directorate, Mascara Province**

Guellali Soria - Djillali Liabés University of Sidi Bel Abbés

guellalisoria@gmail.com

Received: 17/06/2026; Accepted: 13/10/2026

Abstract

The information revolution, which has encompassed the entire world and achieved successes in the development of countries across all sectors and in achieving sustainable development, has made it an indispensable tool or means, as it has come to govern all areas of individuals' lives. Resultantly, many governments, including Algeria, have changed their methods and strategies for conducting their activities and carrying out their work with the aim of providing the best services, through the adoption of the concept of e-business, which utilizes modern technological techniques imposed by the digital revolution. When discussing digitalization, artificial intelligence must be addressed as the foundation for countries' achievement of a significant level of digital development, due to its reliance on an advanced level of modern technology. Nonetheless, the effectiveness of artificial intelligence systems requires the existence of an advanced technological infrastructure and the allocation of specialized financial and human resources with the necessary competence and qualifications in this field, in addition to a legal framework that ensures the safety and security of digital information. The weakness of the legal framework constitutes a threat, resulting in the proliferation and spread of information crime, or what is known as cybercrime. The latter is considered one of the most difficult types of crime due to its difference from traditional crime, as it is an intangible crime. It is difficult to detect and investigate because of its connection to the World Wide Web, on the one hand, and the nature of the perpetrator, who possesses a certain degree of intelligence, skill, and expertise in the field of information technology, on the other hand.

Keywords: Artificial intelligence, legal mechanisms, cybersecurity, cybercrime.

Introduction

The information revolution, which has encompassed the entire world and achieved successes in the development of countries across all sectors and in achieving sustainable development, has made it an indispensable tool or means, as it has come to govern all areas of individuals' lives. Digitalization is considered an integrated system of technical, informational, financial, legislative, human, administrative, political, and social components, it requires the availability of numerous integrated requirements to implement this modern administrative approach and bring it into practical reality, which may face a number of obstacles and risks. Everything has its advantages and disadvantages, and the same applies to

Mecanismos jurídicos para combatir la ciberdelincuencia en la era de la inteligencia artificial

**Organismo responsable: Dirección de Bienes
del Estado de la Provincia de Mascara**

Guellali Soria — Universidad Djillali Liabés de Sidi Bel

Abbés, guellalisoria@gmail.com

Recibido: 17/06/2026 · Aceptado: 13/10/2026

Resumen

La revolución de la información, que se ha extendido por todo el mundo y ha contribuido al desarrollo de los países en diversos sectores y al logro del desarrollo sostenible, se ha convertido en una herramienta indispensable que influye en todos los ámbitos de la vida cotidiana. En este contexto, numerosos gobiernos, entre ellos el de Argelia, han transformado sus métodos y estrategias de gestión con el propósito de ofrecer mejores servicios mediante la adopción de modelos de gestión electrónica que incorporan las tecnologías modernas impulsadas por la revolución digital. El análisis de la digitalización exige abordar la inteligencia artificial como uno de los pilares del avance digital de los países, dada su vinculación con tecnologías de elevada complejidad. No obstante, la eficacia de los sistemas de inteligencia artificial requiere una infraestructura tecnológica avanzada, recursos financieros específicos y personal especializado con las competencias y cualificaciones necesarias, además de un marco jurídico que garantice la protección y la seguridad de la información digital. La debilidad de dicho marco constituye un factor de riesgo que favorece la proliferación de los delitos informáticos, también conocidos como ciberdelitos. La ciberdelincuencia representa una de las formas de criminalidad más complejas debido a su naturaleza intangible, que la distingue de la delincuencia tradicional. Su detección e investigación resultan difíciles tanto por su vinculación con Internet como por el perfil de sus autores, quienes poseen conocimientos, habilidades y experiencia especializados en el ámbito de las tecnologías de la información.

Palabras clave: inteligencia artificial, mecanismos jurídicos, ciberseguridad, ciberdelincuencia.

digitalization, whose widespread adoption and excessive use have led to the proliferation of criminal behavior that may affect information systems and has come to threaten the security of states and even the privacy of individuals. Hence we put the question forward: What are the various legal safeguards and mechanisms established by the Algerian legislator to prevent cybercrime? To answer this question, the first chapter addresses the nature of cybercrime by defining its concept, characteristics, types, and methods of execution. The second chapter then examines the means of preventing and combating it, represented by the establishment of the National Authority for Combating Information and Communication Technology Crimes, as well as procedural mechanisms involving investigation, search and inspection, the infiltration procedure, and blockchain technology.

Topic One: The Nature of Electronic or Cybercrime

The specific nature of cybercrime and its differences from traditional crime require defining its concept and characteristics in the first section, followed by identifying its types and methods of execution in the second section.

Section One: The Concept and Characteristics of Cybercrime

Accordingly, we will address the definition of cybercrime and explain its various characteristics, types, and methods of execution.

Definition of Cybercrime:

Cybercrime is defined as: "All illegal behaviors that use electronic operations targeting the security of the information system and the data it processes" (Djedou, 2022, p. 304).

It is also defined as: "A criminal activity in which electronic technology (computers and the Internet) is used, directly or indirectly, as a means of carrying out the criminal act" (Ali, 2022, p. 194).

It is also described as: "Illegal conduct carried out using electronic devices, resulting in the digital criminal obtaining material and moral benefits. These crimes are often committed through hacking or breaching information systems" (Rawan, 2020, p. 08).

It can also be defined as: "Unlawful, immoral, or prohibited behaviors associated with global information networks. They are considered among the crimes of the digital age, affecting money, knowledge, trust, and reputation, all of which are carried out through technology" (Law No. 06/23, 2006).

However, the Algerian legislator has not used the term "electronic crime" or "cybercrime," but has instead referred to it as "offences affecting automated data processing systems," pursuant to Law No. 04/15 containing the Penal Code (Law No. 04/15, 2004). It was subsequently referred to as "offences related to information and communication technologies" under Law No. 09/04 on the prevention of and fight against offences related to information and communication technologies (Law No. 09/04, 2009), as article 1 of this law defines them: "Offences affecting automated data processing systems as defined in the Penal Code, and any other offence committed or facilitated through an information system or electronic communication systems" (Law No. 09/04, 2009).

On that account, it can be observed that the legislator has confined electronic crime to acts committed through the use of information systems and electronic communication systems. An information system is considered a system, or a set of interconnected systems, that automatically processes data. As for

electronic communication systems, they have been defined as any transmission or communication of signs, signals, writings, images, or other forms of information that are received through any electronic device (Law No. 09/04, 2009).

Moreover, some comparative legal systems have refrained from defining cybercrime, limiting themselves instead to defining information systems and enumerating the functions performed by such systems. These include Jordan and the United Arab Emirates, which are considered among the first Arab countries to adopt information systems legislation.

Jordanian Electronic Transactions Law No. 85 of 2001: Article 2, paragraph 10, defines an information processing system as “the electronic system used to create, send, receive, process, store, or otherwise handle information messages” (Law No. 85, 2001).

Dubai Emirate Electronic Transactions and Commerce Law No. 2 of 2002: This law defines an electronic transactions system as “an electronic system for creating, generating, sending, receiving, storing, displaying, or electronically processing information or messages” (Dubai, 2002).

Characteristics of Cybercrime:

Cybercrime is characterized by several features, including the following:

- Cybercrimes differ in nature from traditional crimes in that the means used to commit them are limited to modern information and communication technologies, represented by computers and mobile phones.
- Cybercrime is intangible and non-material, which makes it difficult to detect due to its connection to the Internet and advanced information technologies.
- Cybercrimes transcend the territorial borders of states, as they constitute criminal conduct committed virtually and are not confined to a specific location.
- Cybercrime requires the perpetrator to possess knowledge and expertise in the field of information technology.
- One of the distinctive features of cybercrime is that it does not require physical strength, as is the case with certain traditional crimes. Instead, such crimes require intellectual ability and mental skills in the digital field (Mahdi, 2021, p. 114).

Section Two: Methods of Committing and Types of Cybercrime

Cybercrime involves the use of methods intended to threaten information security. The Algerian legislator has addressed the types of cybercrime in the Penal Code.

Methods of Committing Cybercrime:

Due to the development of information systems through various modern technological methods, they may be exposed to threats and breaches that penetrate these systems and may even lead to their destruction, potentially resulting in the commission of cybercrime. These methods can be summarized as a range of malicious software programs, which are applications that cause damage to computers, either by slowing down their operation, disabling them, or completely destroying them. They generally include the following:

Viruses: A virus is defined as “a program capable of reproducing itself, that is, replicating and spreading by creating copies (which may be modified) of itself. This is what distinguishes a virus from other malicious programs that do not replicate themselves, such as Trojan horses and logic bombs.” Viruses have evolved over time. Whereas they were once easy to detect, they have become more difficult to identify and can originate from various sources, such as floppy disks and Internet pages, they are further considered destructive programs that target the operating system and computer data (Sawsan, 2011, pp. 394–395).

Trojan Horse: The term “Trojan horse” derives from the wooden horse used by the Greeks to enter the besieged city of Troy and win the war; it is a malicious computer program that disguises itself as a safe program in order to spy on the user and steal information and data from the device. A Trojan horse often comes attached to executable files, particularly free software and email messages. Therefore, caution must be exercised before opening such files, and they should be checked to ensure that they do not contain any dangerous programs.

Spyware: These are programs installed on a computer without its owner's knowledge, making them difficult to detect, they monitor and spy on the device and its user (Hakima, 2021, pp. 657–658), it often originates from advertisements.

Hacking Programs: This refers to gaining unauthorized access to another person's computer by encrypting their data and then illegally infiltrating the system for the purpose of stealing personal information and data, those who engage in such activities are known as “hackers” (Sawsan, 2011, p. 425).

Types of Cybercrime the Algerian legislator addressed offences affecting automated data processing systems in Section Seven bis of Law No. 04-15, which amends and supplements the Penal Code, specifically Articles 394 bis through 394 bis 7. These offences include the following:

- Fraudulent manipulation of all or part of an automated data processing system. Deletion or alteration of system data.
- Insertion, removal, or modification of data within an automated data processing system.
- Designing, researching, collecting, providing, disseminating, or trading in data stored, processed, or transmitted through an information system.
- Possessing, disclosing, disseminating, or using for any purpose data obtained through any of the aforementioned offences.
- Forming a criminal association to commit any of the aforementioned offences.

Attempting to commit the aforementioned offences is punishable by the same penalty prescribed for the completed offence. Furthermore, penalties are doubled when these offences affect a public authority, a public institution, or national defence (Law No. 04/15, 2004).

Topic Two: Methods of Combating Cybercrime

To ensure the security of e-government and protect it against cybercrime, a set of mechanisms has been established to safeguard and ensure information security. These mechanisms are as follows:

Section One: The National Authority for the Prevention of Offences Related to Information and Communication Technologies

The Algerian legislator provided for the establishment of the National Authority for the Prevention of Offences Related to Information and Communication Technologies in Chapter Five of Law No. 09/04, which establishes specific rules for the prevention of and fight against offences related to information and communication technologies. Article 13 thereof states:

- A National Authority for the Prevention of and Fight Against Offences Related to Information and Communication Technologies shall be established.
- The composition, organization, and operating procedures of the Authority shall be determined by regulation” (Law No. 09/04 d. 1., 2009).

The organization of the National Authority for the Prevention of and Fight Against Offences Related to Information and Communication Technologies is also governed by Presidential Decree No. 20-183 (Presidential Decree No. 20-183, 2020), which article 2 of this decree defines it as “an independent administrative authority enjoying legal personality and financial autonomy, placed under the authority of the President of the Republic.”

The powers of the Authority include the following:

- Proposing the components of the national strategy for the prevention of and fight against offences related to information and communication technologies.
- Promoting and coordinating activities aimed at preventing and combating offences related to information and communication technologies.
- Assisting the competent judicial authorities and judicial police services in combating offences related to information and communication technologies, particularly through the collection and provision of information and the provision of judicial expertise.
- Ensuring the preventive monitoring of electronic communications for the purpose of detecting offences related to terrorist and subversive acts and threats to state security.
- Collecting, recording, and preserving digital data from information systems, and identifying its source and path for use in judicial proceedings.
- Ensuring the implementation of requests for assistance received from foreign countries and developing information exchange and international cooperation within its field of competence.
- Developing cooperation with relevant national institutions and bodies concerned with offences related to information and communication technologies.
- Contributing to the training of specialized investigators in technical investigations related to information and communication technologies.
- Contributing to the updating of legal standards within its field of competence.

The National Authority for the Prevention of Offences Related to Information and Communication Technologies is considered one of the most important bodies established by the government to combat criminal conduct of an informational nature. It serves as an investigative body through the search for data and information, in addition to undertaking a range of preventive measures and mechanisms intended to assist the competent judicial authorities, this contributes to facilitating their work, given the considerable difficulty involved in detecting, investigating, and gathering evidence in cybercrime cases.

Electronic Surveillance

The legislator addressed electronic surveillance in Law No. 09-04, in Chapter Two thereof, entitled “Monitoring of Electronic Communications,” by defining it and specifying the circumstances in which electronic surveillance may be used. It defined electronic surveillance as follows: “The use of a computer in the monitoring process in accordance with computer programs specifically designed for this purpose, thereby saving effort, time, and cost in achieving the required results with the least possible losses.” (Nour, 2023, p. 332)

The circumstances that require electronic surveillance are as follows:

- Preventing acts classified as terrorist offences, sabotage offences, or offences affecting state security.
- Where information is available indicating the possibility of an attack on an information system in a manner that threatens public order, national defence, state institutions, or the national economy.
- For the purposes of judicial inquiries and investigations, where it is difficult to reach a result relevant to the ongoing investigations without resorting to electronic surveillance.
- Within the framework of implementing requests for mutual international judicial assistance.

Accordingly, electronic communications may be monitored where there is a possibility that an act constituting a felony or misdemeanor affecting an information system may occur, and where such an act could result in harm to public order, one of the state’s institutions, or its national economy. Over and above, where this circumstance or any of the circumstances stipulated in the aforementioned Law No. 09-04 exists, obtaining written authorization from the competent judicial authority is mandatory (Law No. 09/04 d. 1., 2009).

Special Procedures for the Prosecution of Cybercrime:

Cybercrime is characterized by special prosecution procedures, namely investigation, search, and seizure (Section One); specialized criminal divisions (Section Two); the undercover operation procedure (Section Three); and electronic encryption using blockchain technology (Section Four).

Section One: Investigation, Search, and Seizure

Cybercrime is subject to the same prosecution procedures applicable to traditional crimes. Nevertheless, given the specific nature and importance of cybercrime, the Algerian legislator has introduced exceptions at the stages of criminal proceedings involving preliminary investigations and searches. The general principle stipulates that a person may not be held in police custody for more than 48 hours. However, exceptions apply to certain offences because of their specific nature and importance, including the offence of attacking automated data-processing systems. In such cases, the period of police custody may be extended once, pursuant to written authorization issued by the Public Prosecutor (Article 51 of Law No. 06-22).

Additionally, as a general rule, homes may not be searched before 5:00 a.m. or after 8:00 p.m. Notwithstanding, exceptions apply to certain cases, including offences involving automated data-processing systems, in connection with which searches may be conducted at any time. The territorial jurisdiction of the investigating judge also extends throughout the entire national territory (Article 47 of Law No. 06-22).

The Public Prosecutor may also intercept correspondence, record sounds, and capture images using wired and wireless communication devices. A report must be drawn up specifying the date and time at which these operations begin and end (Articles 65 bis 5 and 65 bis 9 of Law No. 06-22).

In addition, Law No. 09-04 provides that the competent judicial authorities and judicial police officers may search an information system, or part thereof, or the data stored therein, even remotely (Article 05 of Law No. 09-04).

Regarding to the seizure of information relating to cybercrime, the legislator has granted the competent judicial authority the power to seize and copy part, rather than all, of the data contained in an information system, provided that such data are relevant to detecting the offence or identifying its perpetrators. The authority is also required to preserve the integrity of the remaining data within the system (Law No. 09/04 d. 1., 2009).

Be that as it may, if this proves impossible because the competent judicial authorities cannot separate the data related to the offence from the remaining data contained in the information system, they shall seize all the data within the information system by preventing access to or copying of those data (Law No. 09/04 d. 1., 2009).

Specialized Criminal Divisions

Given the characteristics and distinctive features of cybercrime, which set it apart from other offences, particularly because it is among the acts that are difficult to prove and detect due to the offender's intelligence and use of technology to commit the crime, it became necessary to establish a specialized judicial body and appoint judges trained in the field of information technology, with the aim of curbing these serious and complex offences.

The Algerian legislator introduced specialized criminal divisions pursuant to Law No. 04-14, which provides for amendments to the Code of Criminal Procedure (Law No. 04-14). These divisions may be defined as judicial bodies with jurisdiction over specific offences stipulated in Articles 37, 40, and 329 of the Code of Criminal Procedure, including offences affecting automated data-processing systems.

With regard to territorial jurisdiction, specialized criminal divisions are characterized by an extensive scope of jurisdiction, pursuant to the aforementioned Articles 37, 40, and 329, as well as Executive Decree No. 06-348 (Executive Decree No. 06-348, 2016), these provisions allow the territorial jurisdiction of the Public Prosecutor, the investigating judge, and the court to be extended to the jurisdiction of other courts where the matter concerns specific offences exhaustively enumerated by law, namely drug offences, transnational organized crime, offences affecting automated data-processing systems, money-laundering offences, terrorist offences, and foreign-exchange offences.

The Undercover Operation Procedure:

The Algerian legislator introduced the undercover operation procedure as a means of combating modern-day crimes, including offences affecting automated data-processing systems, given their significance and the danger they pose. Further, the Algerian legislator regulated the provisions and rules governing undercover operations in Chapter Five of the Code of Criminal Procedure, from Article 65 bis 11 through Article 65 bis 18.

The Algerian legislator defined the undercover operation in Article 65 bis 12 as follows: “An undercover operation means that a judicial police officer or agent, under the responsibility of the judicial police officer charged with coordinating the operation, monitors persons suspected of committing a felony or misdemeanor by making them believe that he is a perpetrator, accomplice, or receiver of stolen goods alongside them.

For this purpose, a judicial police officer or agent is permitted to use an assumed identity and, where necessary, to commit the acts referred to in Article 65 bis 14 below. Under penalty of nullity, such acts must not constitute incitement to commit offences.” (Law No. 06-22)

For this reason, an undercover operation may be described as an investigative procedure involving the infiltration of criminal activity by a judicial police officer or agent for the purpose of monitoring a person who has committed an act classified as a misdemeanor or felony. Besides, as a formal requirement for the validity of the undercover operation, authorization must be obtained from the investigating authority, namely the Public Prosecutor or the investigating judge, following notification of the Public Prosecutor. (Article 65 bis 11 of Law No. 06-22)

The undercover operation procedure applies to the following offences:

- Drug offences.
- Transnational organized crime.
- Offences affecting automated data-processing systems.
- Money-laundering offences.
- Terrorist offences.
- Offences relating to foreign-exchange legislation.
- Corruption offences (Article 65 bis 5 of Law No.06-22).

Some legislation refers to the undercover operation procedure as “undercover work,” since it involves the use of various methods of impersonation. Through this procedure, the judicial police officer or agent conceals their role in the criminal activity in order to make the perpetrators believe that they are participating in the crime. This procedure also requires the officer or agent to possess a certain level of experience and competence (Mohamed, 1993, p. 110).

The judicial police agent or officer (the undercover operative) must participate in the criminal conduct by:

- “Acquiring, possessing, transporting, delivering, or providing materials, funds, products, documents, or information obtained through the commission of offences or used in their commission.
- Using, or placing at the disposal of the perpetrators of these offences, means of a legal or financial nature, as well as means of transport, storage, accommodation, safekeeping, or communication.” (Article 65 bis 11 of Law No. 06-22)

The undercover operative may act either as a perpetrator, an accomplice, or a receiver of stolen goods.

1. The Undercover Operative as a Perpetrator:

According to Article 41 of the Penal Code, a perpetrator is defined as follows: “A perpetrator is anyone who directly participates in the commission of the offence or incites its commission through gifts, promises, threats, abuse of authority or power, deception, or criminal fraud.” (Law No. 82-04)

2. The Undercover Operative as an Accomplice:

An accomplice is defined under Article 42 of the Penal Code as follows: “An accomplice to an offence is anyone who does not participate directly in its commission but assists or aids the perpetrator or perpetrators by any means in carrying out the preparatory, facilitating, or executing acts, with knowledge thereof.” (Law No. 82-04)

Article 43 of the same Code also specifies the circumstances in which a person is considered an accomplice: “Anyone who habitually provides accommodation, shelter, or a meeting place for one or more criminals who engage in theft or acts of violence against state security, public security, persons, or property, while being aware of their criminal conduct, shall be treated as an accomplice.” (Law No. 82-04)

Pursuant to Article 44 of the aforementioned Code, an accomplice to an offence is subject to the same penalty prescribed for the felony or misdemeanor.

3. The Undercover Operative as a Receiver of Stolen Goods:

Within the meaning of Article 387 of the Penal Code, a receiver of stolen goods is a person who intentionally conceals items obtained through embezzlement or misappropriation, or items originating from an act classified as a felony or misdemeanor (Law No. 66-156).

Finally, it may be said that, despite the seriousness of the undercover operation procedure, as it entails interference with one of the constitutional principles, namely the principle of respect for the privacy of individuals, it is nevertheless considered an important procedure during the investigation and inquiry stage. This is due to the requirements of cybercrime investigations at this stage, particularly the need to uncover the criminal conduct and identify its perpetrators, a task that constitutes one of the difficult operations entrusted to the judicial police.

Electronic Encryption Using Blockchain Technology:

Encryption is one of the techniques used to ensure the security of information and communications, it is not a new technique, as it has been used since ancient times as a means of communication within the military, particularly during wars. Electronic encryption is defined as: “Representations intended to transform readable information into information and signals that cannot be read or understood.” (Mohamed H. A., 2019, p. 249)

As for blockchain technology, it is defined as: “A digital list of records in which transactions are recorded in blocks linked through the use of encryption. When the blocks are filled with data, they are time-stamped and added to the chain of blocks in a manner that can be verified and cannot be altered without the consensus of the participants.” (Haitham, 2021, p. 15)

It is further defined as: “An electronic record created through the use of a decentralized method by multiple parties to verify and store a digital transaction ledger, which is secured through the use of the hash of the information contained in the preceding transaction.” (Haitham, 2021, p. 16)

Accordingly, blockchain technology may be defined as a process through which information is stored in blocks using an encryption mechanism that converts information into fixed symbols, numbers, and letters that cannot be modified (Haitham, 2021, p. 22).

Blockchain serves as a means of authenticating electronic contracts and transactions, as it timestamps all digitally stored information and data, a process referred to as a “timestamp” or “time fingerprint.” (Ashraf, 2020, p. 51)

Blockchain technology also serves as a certification mechanism. Nonetheless, certification through this technology differs from certification in its general sense. Electronic certification is the process carried out by a third party, whether a natural or legal person, who is independent of the parties to the contract, and which involves authenticating electronic transactions. In other words, this party acts as an intermediary (Abed, 2007, p. 70).

The Algerian legislator defined this intermediary in Article 08, paragraph eight, of Law No. 2000-03 as follows: “Any legal or natural person who provides services using wired and wireless telecommunications means.” (Law No. 2000-03, 2000)

Article 02 of Law No. 15-04 also defines it as: “A natural or legal person who issues qualified electronic certification certificates and may provide other services in the field of electronic certification.” (Law No. 15-04, 2015)

In juxtaposition, certification through blockchain technology relies on a peer-to-peer system, through which network participants exchange information and data directly, without an intermediary. Consequently, certification or authentication takes place automatically (Ben Salem, 2022, p. 472).

Accordingly, despite the effectiveness of electronic certification using blockchain technology and the protection it provides through electronic encryption, it is noteworthy that there is no legislative provision through which the Algerian legislator has formally established this mechanism. This is due to the absence of an intermediary responsible for authenticating electronic transactions, which weakens confidence in transactions certified through blockchain technology.

Conclusion

The distinction between digitalization and artificial intelligence has become difficult, as the two complement each other. Every country seeking to enhance and strengthen its infrastructure is therefore required to develop an artificial intelligence strategy. Further, to combat offences related to information and communication technologies, the Algerian legislator has introduced various mechanisms to protect information security and ensure its integrity. Among the most important preventive measures is the establishment of the National Authority for the Prevention and Fight Against Offences Related to Information and Communication Technologies, which serves as an assisting body to the judicial authorities. It collects information and monitors electronic communications in relation to criminal acts involving terrorist and subversive activities and threats to state security. It is also responsible for collecting and preserving data relating to criminal conduct for use as evidence before the competent judicial authorities.

Among the procedural mechanisms for combating cybercrime is the investigation and search procedure, which has characteristics that differ from those of investigation and search procedures in traditional crimes. Given the importance and criminal severity of cybercrime, the legislator departed from the general rule governing police custody, under which detention may not be extended beyond 48 hours, by allowing this procedure to be extended after obtaining written authorization from the Public Prosecutor.

With regard to the search of residences, the general rule stipulates that residences may not be searched before 5:00 a.m. or after 8:00 p.m. However, certain offences are exempted from this rule, including cybercrime, in connection with which searches may be conducted at any time.

Another means of combating digital crimes is the undercover operation procedure, which involves a judicial police officer or agent, under the responsibility of a judicial police officer, monitoring individuals who have committed acts classified as felonies or misdemeanors within the context of cybercrime. The judicial police agent or officer may also assume the role of an undercover operative acting as a principal perpetrator, an accomplice, or a receiver of items relating to an act classified as a felony or misdemeanors.

Blockchain technology is also considered one of the most important modern technologies for combating cybercrime. It operates by storing information in blocks using an encryption mechanism that converts information into symbols, numbers, and letters that cannot be modified.

This technology serves as a means of authenticating electronic transactions, as it enables the timestamping of stored data and information. It also serves as a certification mechanism; however, this differs from certification as defined in Article 02 of Law No. 15-04 concerning electronic signatures and electronic certification. Under the latter procedure, a third party independent of the contract, whether a natural or legal person, is required to act as an intermediary to authenticate electronic transactions between the contracting parties.

Contrastingly, certification through blockchain technology relies on the peer-to-peer principle, whereby the parties to a transaction exchange information and data without an intermediary, allowing the certification process to take place automatically and directly. It is also noteworthy that the Algerian legislator has not expressly provided for blockchain technology, despite its importance. This may be attributed to the absence of an intermediary to authenticate transactions between the contracting parties, which weakens confidence in transactions conducted using this technology.

List of References

1. Abed, F. A. (2007). *Electronic Writing in Civil Law*. Cairo: Dar Al-Nahda Al-Arabiya.
2. Ali, G. a. (2022). Cybercrime: Its Concept and Means of Prevention. *Numerus Economic Journal*, 3(1).
3. Article 05 of Law No. 09-04. (s.d.). same source.
4. Article 47 of Law No. 06-22. (s.d.). previous source.
5. Article 51 of Law No. 06-22, d. 2.-Q. (s.d.). corresponding to December 20, 2006, Official Gazette No. 84, published on December 24, 2006, amending and supplementing Ordinance No. 66-155, dated 18 Safar 1386 AH containing the Code of Criminal Procedure.
6. Article 65 bis 11 of Law No. 06-22. (s.d.). containing the Code of Criminal Procedure, previous source.
7. Article 65 bis 5 of Law No.06-22. (s.d.). containing the Code of Criminal Procedure, previous source.
8. Articles 65 bis 5 and 65 bis 9 of Law No. 06-22. (s.d.). same source.
9. Ashraf, J. (2020). Blockchain and Digital Evidence in the Field of Copyright. *International Journal of Jurisprudence, Judiciary and Legislation*(1).
10. Ben Salem, A. A. (2022, June). An Analytical Comparison of Legal and Technological Frameworks. *Journal of Legal and Political Studies*, 8(2).
11. Djedou, B. A. (2022, July). Cybersecurity Challenges in Confronting Cybercrime. *Algerian Journal of Human Security*, 7(2).
12. Dubai, E. L. (2002, February 12). concerning electronic transactions and commerce.
13. Executive Decree No. 06-348, d. 1. (2016, October 17). determining the territorial jurisdiction of certain courts, Public Prosecutors, and investigating judges, Official Gazette No. 63.
14. Haitham, E.-S. A. (2021). *The Emergence of Smart Contracts in the Blockchain Era* (éd. 1). Cairo: Dar Al-Nahda Al-Arabiya for Publishing and Distribution.
15. Hakima, D. (2021). The Implications of Cybercrime on the Digital Environment: A Study of Mechanisms and Strategies for Combating It. *Annals of the University of Algiers* 1, 35(3).
16. Law No. 04/15, d. N. (2004, 10). amending and supplementing Law No. 66/156 relating to the Penal Code, Official Gazette No. 71,, as amended and supplemented.
17. Law No. 04-14, d. 2.-1. (s.d.). containing the Code of Criminal Procedure.
18. Law No. 06/23, d. D. (2006, December 24). amending and supplementing Law No. 66/156 relating to the Penal Code, Official Gazette No. 84,.
19. Law No. 06-22. (s.d.). containing the Code of Criminal Procedure, previous source.

20. Law No. 09/04, d. 1. (2009 , August 16). establishing specific rules for the prevention of and fight against offences related to information and communication technologies, Official Gazette No. 47.
21. Law No. 09/04, d. 1. (2009, August 16). concerning specific rules for the prevention of and the fight against crimes related to information and communication technologies, Official Gazette No. 47.
22. Law No. 15-04, d. 1.-T. (2015, February 10). establishing the general rules relating to electronic signatures and electronic certification.
23. Law No. 2000-03, d. 0.-A. (2000, August 6). establishing the general rules relating to the postal service and wired and wireless telecommunications.
24. Law No. 66-156. (s.d.). Article 387 of the Algerian Penal Code.
25. Law No. 82-04, d. F. (s.d.). amending and supplementing Ordinance No. 66-159.
26. Law No. 85, o. 2. (2001, December 31). Official Gazette of the Hashemite Kingdom of Jordan No. 4524.
27. Mahdi, R. (2021). Cybercrime and Mechanisms for Combating It under Algerian Legislation. *Eliza Journal of Research and Studies*, 6(2).
28. Mohamed, A. M. (1993). *Covert Operations in Combating Drug Trafficking*. Riyadh: Arab Center for Security Studies and Training Publishing House.
29. Mohamed, H. A. (2019). *Proof of the Electronic Administrative Contract*. Alexandria: Dar Al-Jamia Publishing House.
30. Nour, E. H. (2023). Cybercrime and Mechanisms for Combating It: Addressing Cybersecurity Challenges. *Algerian Journal of Law and Political Science*, 8(1).
31. Presidential Decree No. 20-183, d. 2.-Q. (2020, July 13). concerning the reorganization of the National Authority for the Prevention of and Fight Against Offences Related to Information and Communication Technologies.
32. Rawan, b. A.-S. (2020, May). Cybercrimes. *Comprehensive Multidisciplinary Electronic Journal*(24).
33. Sawsan, Z. A.-M. (2011). *E-Government Technology* (éd. 1). Amman, Jordan: Dar Osama for Publishing and Distribution.