

Contemporary cybercrime challenges and legal responses in Algerian legislation

التحديات الراهنة للجريمة الإلكترونية وسبل مواجهتها في التشريع الجزائري

ACHIR Djilali*, The legal system of contracts and actions in private law Laboratory
University of khemis milliana

d.achir@univ-dbkkm.dz

.Gachi Allel, The development policies and prospective studies Laboratory
University of Ali Lounici-Blida2-

a.gachi@univ-blida2.dz

Received: 29/09 /2025

Accepted: 13/11 /2025

Published: 29/11 /2025

Abstract:

Cybersecurity has evolved into a fundamental necessity for all nations, serving as a critical pillar of modern security systems. Governments entrust various security agencies with safeguarding digital infrastructure, especially amid the rapid rise of cybercrime. The expansion of transnational cybercriminal networks has introduced complex challenges, necessitating robust legal and legislative measures to mitigate risks.

This research begins by clarifying the concept of cybercrime, exploring its definition in jurisprudence generally, and in comparative law particularly. It then identifies the main characteristics and types of cybercrimes, After that the study turns to the legal response to these crimes in the Algerian context, focusing on both **substantive legal protections** and **procedural protections**

Key words: Electronic crime - objective protection - procedural protection - information system - stakes.

introduction:

Societies have witnessed profound advancements across all domains—political, economic, cultural, and even criminal. Traditional crimes have transformed, adapting to modern contexts. Technological progress, particularly in the digital sphere, has undeniably benefited individuals and institutions. Yet, these advancements have also facilitated the emergence of some of the most dangerous and sophisticated crimes today: **cybercrime**.

The importance of addressing cybercrime is paramount, as it represents one of the most pressing and contemporary issues facing the global community. On a theoretical level, studying this phenomenon helps us understand the nature of cybercrimes, how they differ from traditional offenses, and how legal systems attempt to regulate them. On a practical level, such understanding is essential to protecting individuals and institutions in Algeria from falling victim to these harmful digital threats.

This research seeks to answer two central questions:

What is cybercrime? And how does Algerian legislation address and confront it?

Significance of the study:

This study aims to highlight cybercrime and its contemporary challenges, as well as to emphasize the legal methods for preventing it.

* Corresponding Author

” The recent challenges of cybercrime and the ways to deal with them in the algerian legislation”

Objectives:

- Clarifying the Concept of Cybercrime in Light of Jurisprudence, Law, and Arab and Western Legislation
- Identifying the Characteristics of Cybercrime and Distinguishing It from Traditional Crime
- Outlining the Major Challenges of Cybercrime Facing Countries and the Possibility of Providing Substantive and Procedural Protection to Avoid the Risks of This Crime.

Methodology:

For studying our topic and addressing the problem statement, we followed the analytical method as it is the most suitable for analyzing legal texts related to cybercrime and outlining ways to confront it. Additionally, we employed the descriptive method, focusing on describing the newly emerging crime with all its characteristics.

Research plan:

Handling this issue necessitates two sections. The first section includes the concept of cybercrime, with two subtopics under it. The second section covers the challenges of cybercrime, also with two under it.

Section I : The Concept of Cybercrime

Section II : Challenges of Cybercrime

Section I :The Concept of Cybercrime

There is a clear global trend toward digital governance that follows rapid technological developments. In the Arab world, especially in the countries of the Arab Maghreb, growing cybersecurity threats have raised serious regional and international concerns. As a result, researchers have focused on clearly defining cybercrime and identifying its key characteristics. The goal is to help develop legislation that effectively address the nature of these crimes and their impact on societies and nations.

1-The First Requirement: Definition of Cybercrime

Understanding cybercrime and its legal nature requires familiarity with both its conceptual meaning and legal definitions in jurisprudence.

1.1-Terminological Definition of Cybercrime

Cybercrime refers to criminal activities carried out using computers, digital devices, or the internet. Unlike traditional crimes, which often involve physical violence, cybercrime is sometimes referred to as a "crime of the intelligent" because it requires technical knowledge and is carried out in non-physical ways. It involves the deliberate use of digital tools to access, manipulate, or destroy information systems. This type of crime reveals both similarities and contrasts with conventional forms of criminal behavior.

1.2-Definition of Cybercrime in Jurisprudence

Jurists generally classify definitions of cybercrime into two main categories: a narrow definition that limits it to crimes targeting computer systems, and a broad definition that includes any crime committed using digital technologies.

1.2.1- The narrow definition

Some jurists define cybercrime as “any unlawful act involving a computer.” Others offer more specific definitions, such as “any crime against public funds committed through automated information processing.”

According to supporters of the narrow approach, cybercrime refers to “any unlawful act where significant knowledge of computer technology is necessary for both its commission and investigation.” It is also described as “criminal activity that primarily uses a computer as a tool.” This view limits cybercrime to offenses involving direct interference with computer systems, including the unauthorized duplication, modification, deletion, or access of data stored or transmitted through digital networks.

” The recent challenges of cybercrime and the ways to deal with them in the algerian legislation”

1.2.2- The broad definition

Jurists such as Michel and Credo adopt a broad interpretation of cybercrime, defining it as the use of computers as tools to commit various offenses. This includes unauthorized access to a victim's computer or data, attacks targeting computer systems or connected devices, and crimes where computers are not the direct target but serve as instruments in the commission of the offense.

Examples under this broad view include unauthorized use of credit cards, tampering with ATMs, and misuse of electronic banking networks. It also extends to the theft of computers or their components, and the manipulation of both physical and digital elements of computing systems. This comprehensive perspective aligns with the definition adopted by the Tenth United Nations Congress on Crime Prevention and Criminal Justice, which has been reflected in Algerian legal thought. According to this definition, cybercrime encompasses any criminal activity that occurs within, through, or by means of a computer network. Essentially, it includes all crimes that can be committed in a digital environment.

1.3-Cybercrime: Legal Definition

Although the task of defining cybercrime traditionally falls within the domain of legal scholarship and jurisprudence, legislators around the world have shown increasing interest in establishing legal definitions of this phenomenon. The diversity of perspectives on cybercrime has led to a range of definitions found in various legal systems. Therefore, this section presents selected definitions from both Western and Arab legislation that attempt to legally characterize cybercrime.

1.3.1- The definition according to Saudi legislation.

Under the Anti-Cybercrime Law of the Kingdom of Saudi Arabia, an **information system** is defined as: *“A set of programs and tools designed for processing and managing data, including computers.”*

1.3.2- the definition according to French legislation

The French Law No. 88-19 of 1988 defines types of cybercrime and distinguishes between attacks on computer programs and data, and attacks on computer tools and machines. It does not explicitly criminalize the theft of programs and information, considering it non-property crime¹.

1.3.3- The definition according to Algerian legislation

In contrast to the French legislator, the Algerian legislature did not define cybercrime until recently. This definition appears in Article 2, paragraph 1 of Law No. 09-04, dated 14 Sha'ban 1430 (corresponding to August 5, 2009). This law, published in Official Gazette No. 47 on August 16, 2009, sets out specific provisions for the prevention and prosecution of offenses involving information and communication technologies.

According to Article 2, paragraph 1 of Algerian Law No. 09-04: **"Crimes involving interference with data processing systems, as defined in the Penal Code, and any other crime committed or facilitated through an information system or electronic communications system."**

The information revolution and the emergence of new forms of criminality—unprecedented in human history—have prompted Algerian legislators to criminalize interference with computer systems. Articles 394 bis through 394 bis 07 of the Algerian Penal Code set out the specific provisions related to such offenses. On July 26, 2001, Law No. 01-09, the first piece of legislation addressing cybercrime in Algeria, was incorporated into the Penal Code. It introduced provisions found in Articles 144 bis, 146, 144 bis 1, and 144 bis 2 of the Penal Code, which specifically address offenses such as insulting or defaming the President of the Republic, the Islamic religion, government institutions, or public officials.

In contrast to other legal systems, Algerian legislation defines automated data processing systems by emphasizing the necessity of connections between system devices or components, or

” The recent challenges of cybercrime and the ways to deal with them in the algerian legislation”

between entire systems. By focusing on the intended function of automated data processing, the definition broadens its scope to include all forms of such processing activities.

2-Characteristics and Types of Cybercrime

Cybercrime possesses several distinctive characteristics due to its unique nature. One of its primary features is the absence of geographical boundaries, allowing it to be committed from virtually anywhere in the world. It is often perpetrated by highly skilled individuals capable of infiltrating, modifying, adding to, or even completely disabling information systems. Moreover, cybercrime encompasses a wide range of offenses, making it a diverse and constantly evolving threat.

2.1-Cybercrime Features

Certain characteristics set cybercrime apart from regular crime. Among these qualities are :

2.1.1- Cybercrime is Transnational

Cybercrime is international in scope due to the global connectivity provided by the internet. It does not respect national borders, which makes it a modern form of transnational crime. A wide range of offenses can be carried out through information systems, such as data breaches, document forgery, fraud, hacking, and financial theft.

Because of the serious global threat posed by cybercrime and the significant damage it causes, international cooperation has become essential. One notable example is Interpol's efforts in this field. The organization deploys specialized officers across various countries who help build and maintain a global database. This database serves as a vital tool for tracking and responding to cybercrime.

2.1.2- Difficulty in Proving Cybercrime

Cybercrime is marked by its hidden nature. Unlike traditional crimes, it often leaves no physical traces, making detection and investigation particularly challenging. Offenders operate in a virtual, technological environment where illegal actions—such as data breaches or manipulation—occur without visible, physical consequences. The vast amount of data and the global scale of the internet further complicate efforts to trace these crimes.

Several factors contribute to the difficulty in combating cybercrime:

- **Lack of physical evidence:** Cybercrime takes place in a digital environment where no tangible documents are exchanged. Information is transmitted through invisible electronic signals, leaving behind little to no trace once the crime is committed.
- **Intangible and complex nature:** As a relatively new form of crime, cybercrime is difficult to identify or reconstruct. It often leaves no material evidence or witnesses that traditional criminal investigations rely upon.
- **Technical complexity:** Investigating cybercrime requires a high level of technical expertise. Conventional law enforcement agencies may lack the specialized knowledge in computer technologies and information systems needed to track, analyze, and prosecute these offenses.
- **Underreporting by victims:** Many victims, particularly financial institutions, are reluctant to report cybercrimes. Fearing reputational damage and loss of customer trust, they may choose not to cooperate with investigative authorities, resulting in widespread underreporting.

2.1.3- Cybercrime is Quickly Executed

One of the defining features of cybercrime is the speed at which it can be carried out. In many cases, a single keystroke is enough to transfer millions of dollars, steal sensitive data, or disrupt critical systems. Cybercrimes often require minimal time to execute, and unlike traditional crimes, they generally do not involve elaborate planning or the use of physical tools.

Moreover, most cybercrimes—aside from the physical theft of computer hardware—do not require the offender's physical presence at the crime scene. A perpetrator can commit an offense remotely, from anywhere in the world, simply by gaining access to a network. This enables acts

” The recent challenges of cybercrime and the ways to deal with them in the algerian legislation”

such as intercepting financial transactions, stealing confidential information, or launching damaging attacks, all without crossing borders or being physically detected.

2.1.4- It Requires Technical Expertise

Due to its highly technical nature, cybercrime demands specialized knowledge and proficiency in information technology. Traditional law enforcement personnel may lack the necessary skills to investigate such crimes effectively. Handling cybercrime cases requires investigators who are specifically trained in digital forensics and cybercrime procedures to ensure that electronic evidence is properly identified, preserved, and analyzed. Without this expertise, there is a significant risk of compromising or even destroying crucial evidence during the investigation process.

2.1.5- The reason behind cybercrime

The motivations behind cybercrime often differ from those of traditional crimes. These offenses are typically committed without direct contact with the victim and may be driven by a variety of factors. Common motives include financial gain, the desire to defame or discredit individuals or institutions, attempts to exert influence or manipulate public opinion, or simply a disregard for legal and ethical norms. In many cases, offenders exploit digital platforms to achieve their objectives while remaining anonymous and avoiding immediate detection.

2.2-Cybercrime Types

Cybercrime affects people and morality in every field and domains, including the political, cultural, and economic. Among the instances are:

2.2.1- Material Crime

This category of cybercrime results in financial loss or material damage to the victim. It typically takes one of the following forms:

- **Electronic Theft:** Common in many countries, these crimes involve unauthorized access to bank accounts or ATMs. Offenders often duplicate electronic data from ATM cards to withdraw funds.
- **Creating a Fake Online Identity:** This involves designing fraudulent websites that closely imitate official platforms of banks or financial institutions to deceive users.
- **Phishing Emails:** Messages from unknown sources attempt to scam recipients by promising lottery winnings or soliciting donations, often in exchange for a portion of a supposed larger sum.

2.2.2- Crimes Against Individuals

Cybercrime can target individuals directly through electronic systems. Although less frequent in practice, this category includes:

- Defamation, slander, and insult
- Unauthorized disclosure of personal or commercial secrets
- Threats, incitement, and invasion of privacy via the internet

2.2.3- Moral Crimes

The problem of morality on the internet has taken up a lot of space in comparative jurisprudence research since various countries have different moral standards. Crimes that violate established moral standards in socioeconomic contexts are classified as moral crimes. Important cases include offenses against the sanctity of private life, crimes involving sexual exploitation, and offenses involving libel, insulting, and defamation².

2.2.4- Economic and Political Crime

The internet's ability to simplify communication has been used by numerous extremist organizations to share their ideas and views. This has progressed to actions that threaten the safety of states that are the targets, especially through organized crime and terrorism, which have gained new dimensions as a result of internet use. They can now perpetrate crimes against nations and communities thanks to the internet. Even more dangerously, especially in nations where there are

” The recent challenges of cybercrime and the ways to deal with them in the algerian legislation”

typical conflicts, the internet has made it possible for many countries to acquire the military and economic secrets of other countries and conduct espionage against them³.

2.2.5- Crimes against Culture

Cultural crime can take one of the following forms, when the offender appropriates intellectual property rights without the victim's consent:

- Software theft is the practice of copying or repurposing software from foreign businesses onto disks and reselling them for cheaper prices.
- Unauthorized Access to Encrypted Satellite Channels: Using soft copy technology to make encrypted satellite channels accessible online.
- Copies of Literary and Scientific Works Using Current Electronic Techniques⁴.

Section II :Challenges of Cybercrime

Countries around the world face significant challenges in addressing cybercrime. These crimes often transcend national borders and are carried out rapidly, making detection and prosecution more complex. To effectively combat cybercrime, both **substantive** and **procedural** protections must be in place to safeguard information systems and minimize associated risks.

1- Substantive Protection of Information Systems

Information today holds substantial economic value, making it a key asset in both public and private sectors. Because of its importance, information requires strong legal protection—especially when its unauthorized access or disclosure can harm individuals or compromise economic interests.

1.1-Protection under Intellectual Property law

Intellectual property rights refer to moral ownership rights that pertain to non-material items and are divided into three types:

- **Industrial Property Rights:** These pertain to new innovations that allow their owner to exclusively exploit the innovation before anyone else. They include: Rights related to new innovations in terms of the shape and external appearance of products (designs, patterns, or industrial models). Rights related to new innovations in terms of the subject matter, such as inventions. Rights pertaining to distinctive signs that allow their owner to exclusively use a mark to distinguish establishments, like commercial trademarks.
- **Commercial Property Rights:** These include the rights a merchant has over their commercial establishment, considering it as movable property.
- **Literary and Artistic Property Rights:** These refer to the rights an author has over their intellectual production in literature, arts, and sciences.

To protect intellectual works, the Algerian legislator has established general conditions, which include the existence of the work itself and its compliance with public order. Additionally, there are specific conditions, such as the presence of a new innovation in the work and the legal deposit of the work⁵.

1.2-Protection under the Penal Code

Traditional criminal law often struggles to keep pace with technological advances. Most legal provisions were established before the digital age, and therefore do not fully address modern cyber offenses. Recognizing this gap, the Algerian legislator introduced **Law No. 04-15**, which amends the Penal Code to include provisions targeting cybercrime.

1.2.1- Criminalization of Attacks on the Data Processing System

The Algerian legislator defines a data processing system as: **“Any system or group of systems, whether separate or interconnected, where one or more systems perform automatic data processing according to a specific program.”** This definition aligns with that adopted by the **Budapest Convention on Cybercrime**, the leading international treaty in this domain. The existence of such a system is a fundamental prerequisite for establishing that a cyberattack has taken place.

” The recent challenges of cybercrime and the ways to deal with them in the algerian legislation”

1.2.2- Criminalization of Attacks on Data within the Systems

In this context, an "attack" refers to any action aimed at compromising the **confidentiality**, **integrity**, or **availability** of data stored or processed within the system. These attacks may result in the alteration, deletion, or corruption of data, and often follow a prior act of unauthorized access. The objective is usually to impair the normal functioning of information systems or to manipulate their outputs for illicit purposes.

1.2.3- Attacks on the Operation of Data Processing Systems

Although the Algerian legislator does not explicitly criminalize attacks on the **operation** of data processing systems, such offenses can be inferred from the broader provisions introduced by **Law No. 04-15**. For example, **Article 393 bis** penalizes acts of sabotage, which by their nature impair or disable the functionality of the system. Similarly, introducing malicious software such as viruses or logic bombs may disrupt the system's operation, indirectly falling under offenses targeting internal data or the integrity of the system itself. These forms of attacks affect the system's ability to function reliably and securely.

1.3-Protection under the Law on the Prevention of Crimes Related to Information and Communication Technologies:

Law No. 09-04, issued on August 5, 2009, contains 19 articles divided into six chapters. The law includes specific provisions for electronic surveillance, which can only be conducted with the permission of the competent judicial authority and in certain cases. These cases include acts described as terrorism and sabotage, crimes affecting state security, or situations where there is information about a potential attack that threatens the information systems of state institutions, national defense, or public order. The law establishes a National Agency for the Prevention and Combat of Crimes Related to Information and Communication Technologies. This agency is responsible for initiating and coordinating prevention operations against cybercrime and assisting judicial police services in their investigations of such crimes. The agency is also tasked with exchanging information with its counterparts abroad, emphasizing the principle of international cooperation based on reciprocity. Law No. 09-04 is considered comprehensive in the field of combating cybercrime, as it criminalizes unlawful acts committed via communication means in general. Therefore, it applies to all new and old technologies, including the internet, and any future technologies that may emerge.

2- Procedural Protection of the Information System:

In addition to establishing penal protection through substantive legal provisions, the Algerian legislator has introduced a series of measures aimed at ensuring special protection for information systems. These measures include procedures for investigating cybercrime and collecting electronic evidence.

2.1-Investigating Cybercrime

The investigation process is essential for proving that a crime has occurred and for establishing evidence against the perpetrators using various forms of proof. As the name suggests, its purpose is to uncover the truth and determine the guilt or innocence of the accused after collecting the relevant evidence.

2.1.1- Authorities Responsible for Cybercrime Investigations

Cybercrime investigations may be conducted by various legal authorities. These include **judicial police officers**, **members of the public prosecution**, and **investigating judges**. The **criminal investigator**, who is usually a member of the judicial police, plays a central role. The law grants them the responsibility of collecting and securing evidence related to suspected criminal activity.

2.1.2- Characteristics of cybercrime Investigations and Investigators

Because cybercrime investigations rely on electronic methods, they have unique procedures. The way these investigations are done and the investigator's role are different from traditional criminal cases.

” The recent challenges of cybercrime and the ways to deal with them in the algerian legislation”

2.1.2.1- Characteristics of Electronic Investigation

Electronic investigations have unique features, whether done during a preliminary inquiry or an initial technical assessment. They often need experts with advanced technical skills to track digital activity, secure electronic evidence, and analyze data. Unlike traditional investigations, they don't depend on physical clues but on digital traces, metadata, and encrypted information, which require accuracy, speed, and confidentiality.

2.1.2.1.1- Method of Preliminary Investigation

- **Developing an Investigation Plan:** The plan is developed based on the information available to the investigator and involves identifying the technical team required to assist with the case. It is implemented only after inspecting the crime scene, evaluating the system's security infrastructure, identifying the source of the threat, and outlining strategies to counter the attack. The technical planning stage focuses on determining the most effective methods to address the crime in a detailed and organized manner. This is followed by a thorough and coordinated review of all investigative procedures, as discussed and approved by the investigation team.
- **Forming the Investigation Team:** The team must consist of technicians and specialists with extensive knowledge of computers and internet systems to combat this criminal activity. This expertise is only achieved after receiving adequate education and training in information technology and knowledge of foreign languages. The team includes the lead investigator, computer and internet network experts familiar with the incident's circumstances and how to handle such crimes, experts in handling and processing digital evidence, computer systems experts who deal with software systems, and experts in photography, fingerprints, and sketching⁶.

2.1.2.1.2- Investigation Procedures

Before starting the preliminary investigation, certain prior procedures must be observed:

Preliminary Procedures Before Starting the Investigation:

- **Identifying the Type of Automated Data Processing System:** Determine the specific system involved in the crime.
- **Creating a Detailed Plan of the Facility:** Map out the location where the crime occurred.
- **Considering the Difficulty of Preserving Evidence:** Recognize that electronic evidence may not last long.
- **Considering Potential Interference by the Perpetrator:** Be aware that the perpetrator may destroy stored information through the network.
- **Disconnecting Electrical Power:** Cut off power to the site to prevent the perpetrator from erasing evidence.
- **Disconnecting Telephone Lines:** Prevent misuse of phone lines by the perpetrator and confiscate mobile phones from unrelated individuals.
- **Verifying the Phone Line Used:** Ensure the phone line belongs to the computer involved in the crime.
- **Keeping Employees Away from Computers:** Remove access to computers from employees after the perpetrator has obtained the password.
- **Photographing the Targeted Devices:** Document the devices involved in the crime with photographs.

Procedures During the Investigation:

- **Creating Backup Copies:** Make backup copies of hard drives or floppy disks before using them and verify the accuracy of the copies technically.
- **Removing the Computer Cover:** Open the targeted computer and check for additional hard drives.

” The recent challenges of cybercrime and the ways to deal with them in the algerian legislation”

- Analyzing Disk Content: The goal of copying disk content is to analyze the information to identify deleted files.
- Examining Software and Applications: Inspect the programs and their applications.
- Investigating the Relationship Between Applications and Files: Focus on the interaction between applications and files, particularly those involving data entry and output.
- Preserving Seized Equipment: Store the equipment and devices seized in a technically sound manner⁷.

2.1.2.2- Characteristics of the Electronic Investigator

The technical characteristics include:

- **Technical Knowledge** : Understanding the technical and technological aspects of computers and the internet.
- **Legal Procedures**: Knowing how to quickly and legally preserve electronic evidence.
- **System Knowledge**: Being familiar with how computers and networks are set up.
- **Understanding Different Systems**: Knowing about various computer systems
- **Data knowledge**: Knowing file formats and their contents.
- **Awareness of Cybercrime and Security**: Recognizing the methods used to commit cybercrimes and the techniques of information security⁸.

2.1.2.3- Suitable Evidence for Proving Cybercrime

Evidence is any trace or fact that comes from the crime itself. For example, forgery is proven by showing that a document's truth has been altered. In cybercrime cases, evidence is found through technical means, using the same tools that were used to commit the crime. This is called digital evidence, which exists in virtual spaces.

Digital evidence comes from computer systems and appears as data, magnetic signals, or electrical pulses. It can be collected and analyzed using special software and must be presented in a way that a court will accept. In short, it is evidence based in the virtual world that helps prove and identify the crime.

2.2- Electronic Evidence

The procedures for collecting electronic evidence are divided into traditional methods and modern methods:

- **Traditional methods**: These include physical actions such as inspection, search, and seizure, as well as personal actions like testimony and expertise.
- **Modern methods**: saving data, intercepting communications, recording audio, taking images, and infiltration.

The modern methods will be explained in detail later

2.2.1- Traditional Procedures for Collecting Electronic Evidence

Collecting electronic evidence requires following traditional physical procedures such as inspection, search, and seizure, as well as traditional personal procedures like expertise and testimony.

2.2.1.1- Physical Procedures

2.2.1.1.1- Inspection:

Inspection is an investigative step done by the investigating authority itself or by judicial police officers. The court can also order an inspection if it is needed to uncover the truth, either on its own or at the request of a concerned party, with the judge's approval.

When investigating a cybercrime scene, it should be seen as having two parts:

- **The Traditional Scene**: This includes the physical parts of the crime location, like devices, storage media, or physical evidence left behind, similar to fingerprints or personal items at a traditional crime scene.

” The recent challenges of cybercrime and the ways to deal with them in the algerian legislation”

- **The Virtual Scene:** This covers the digital data stored on devices or online, such as files on hard drives or data in cloud storage.

Because cybercrime scenes are different from other crime scenes, they need special handling and technical steps to secure evidence properly before starting the investigation.

- **2.2.1.1.2- Search:** An electronic search is an investigative step carried out by the judicial police under a warrant in special cases. It aims to find digital evidence on computers or smart devices. Searching and seizing computers or storage systems is a key method for uncovering cybercrimes.

2.2.1.1.3- Seizure: In cybercrime cases, seizure covers both intangible and physical items. This includes data, electronic communications, and emails, as well as physical items like paper documents, computers, peripherals, internal and external hard drives, optical discs, and magnetic cards.

2.2.1.2- Personal Procedures

2.2.1.2.1- Expertise: The expert must have the right scientific and technical knowledge for the case and be able to work effectively. Their tasks include locating possible evidence, describing what it looks like, assessing any financial or economic impacts, and deciding how to isolate a system when needed without damaging evidence or equipment.

2.2.1.2.2- Testimony: This is provided by a digital witness, also known as an information technology expert. This individual is a specialist with expertise in computer science and technology, possessing essential knowledge required to access data processing systems. Digital witnesses typically fall into several categories, including: computer operators, programming experts, analysts, maintenance and communications engineers, and system administrators⁹.

2.2.2- Modern Procedures for Collecting Electronic Evidence

2.2.2.1- Data Preservation

Algerian law requires service providers to collect, store, and organize certain types of data. Searches and other legal steps may also be used to secure this data. The law clearly states what kinds of data must be kept, focusing on traffic data (information about digital communications). According to Article 11 of Law 09-04, service providers must keep:

- Data that identifies users.
- Data about the communication equipment used.
- Technical details, including the date, time, and duration of each connection.
- Data about any extra services used and their providers.
- Data that identifies recipients, connections, and websites visited.

Because data preservation is only temporary, and to protect privacy rights, Algerian law requires service providers to delete this stored data one year after it is recorded. Service providers act as a source for investigators to get digital evidence from the preserved data and must provide it when asked.

2.2.2.2- Intercepting Communications, Recording Audio, and Capturing Images

Intercepting communications means capturing, recording, or copying messages that can be produced, sent, stored, received, or displayed. This includes both wired and wireless communications when investigating and collecting evidence for crimes.

Algerian law, under Article 65 bis 5 of the Code of Criminal Procedure, sets out how and when this can be done. It allows investigators, when needed for ongoing criminal or cybercrime cases, to intercept wired and wireless communications, record conversations and sounds, and capture images.

2.2.2.3- Infiltration

Infiltration is defined in Article 65 bis 12 of the Algerian Code of Criminal Procedure No. 06-22. It applies to crimes involving automated data processing systems. Infiltration allows a police officer or judicial police agent to enter the virtual world — for example, by joining chat rooms,

” The recent challenges of cybercrime and the ways to deal with them in the algerian legislation”

online forums, or direct communications — to observe and understand how people might hack networks or spread viruses.

The officer can use a false identity or a fake organization name to appear as a regular participant. This helps investigators uncover and catch criminals.

Conclusion:

Advancements in modern technology have brought many conveniences to daily life but have also created new opportunities for cybercrime, making its investigation and prevention increasingly challenging. This has driven lawmakers and governments to develop specific procedures to address and combat these crimes.

From our study, we reach the following conclusions:

- Cybercrime threatens the safety and security of individuals and society because of its hidden nature and the high level of professionalism of its perpetrators.
- Algerian legislation has not yet established a law dedicated solely to cybercrime.
- Despite ongoing efforts, significant control over cybercrime has not yet been achieved.
- Existing laws and regulations are outdated and do not keep pace with the constant evolution of cybercrime.

Key Recommendations:

- Learn from the experiences of more advanced countries in these areas, as they possess more expertise in combating cybercrime.
- Monitor electronic communications, messages, and activities similarly to mobile phone communications to reduce incidents of cybercrime.
- Conduct awareness campaigns and educational programs to highlight the dangers of cybercrime and prevent its occurrence.

References:

-
- ¹ Mohamed Mustafa Moussa, Investigating Cyber Crimes, police presses, Cairo, 2009, pp. 118-119.
 - ² Fatemah Zahra Bkhi, Procedures for Investigating Cybercrime, Master's thesis in Law, Mohamed Boudhief University, M'sila, 2013/2014, p. 27.
 - ³ Ismahan Boudiaf, Cybercrime and Legislative Procedures for Addressing It in Algeria, professor researcher journal for legal and political studies, Mohamed Boudiaf University, M'sila, volume 3, Issue 3, 2018., p. 358.
 - ⁴ Mohamed Bouamra, Said Ali Bounenal, Same Reference, p. 11.
 - ⁵ Aicha Naïri, Same Reference, p. 36.
 - ⁶ Youssef Jaffal, Same Reference, p. 41.
 - ⁷ Youssef Jaffal, Same Reference, p. 42.
 - ⁸ Youssef Jaffal, Same Reference, p. 43.
 - ⁹ Saida Baara, Same Reference, p. 82.