MAPAN-JOURNAL ,
Publisher: METROLOGY SOC INDIA , NPL PREMISES,
Address: DR K S KRISHNAN MARG, NEW DELHI, INDIA,
ISSN / eISSN:0970-3950 / 0974-9853
Volume 25-Issue 1-(2025)
https://doi-001.org/1025/17615906785867

OPEN ACCESS

International and National Legal Challenges in Combating Electronic Financial Crimes

Mekkaoui Zoubeyr

Senior Lecturer, Class A
Faculty of Law and Political Science, Tahri Mohamed University of Béchar, Algeria
Research Laboratory for Legal Studies and Professional Responsibility

Email : mekkaoui.zoubir@univ_bechar.dz

Received : 11/04/2025 ; Accepted : 27/08/2025

ABSTRACT

Electronic financial crimes are global and transnational offenses. They are highly complex and interconnected crimes that occur on both physical and virtual levels. Therefore, cooperation between various security agencies at the global and regional levels is required now more than ever to confront the legal and security challenges posed by these crimes. This has led some countries to establish specialized departments within their security and administrative institutions to combat electronic financial crime. These institutional mechanisms are not limited to the national level but also extend to the regional and even international levels.

Keywords: Electronic financial crimes, legal challenges, regional and international security agencies.

INTRODUCTION

There is no doubt that the increasing forms and magnitude of losses and damages resulting from electronic crimes, especially financial ones, which have often affected states and major financial institutions, have proven in practice that no country can, through its individual efforts, confront electronic crime. Therefore, countries have sought to unify their efforts to combat it. Consequently, addressing this issue requires joint international cooperation to establish appropriate mechanisms to confront this phenomenon.

Electronic crime knows no territorial, geographical, or political boundaries. Such crimes may be committed across different parts of the world within minutes. The existence of institutional mechanisms dedicated to combating electronic crimes constitutes an important deterrent means against criminal acts committed in the information society. These mechanisms may reduce the occurrence of electronic crimes and contribute to limiting them, not to mention the significant role played by preventive mechanisms in curbing and preventing such crimes even before they occur.

Accordingly, the study of institutional mechanisms and international and national efforts to combat electronic financial crimes focuses on the international and national confrontation of these crimes. This article addresses the **international and national legal challenges in combating electronic**

financial crimes through the following main question: *What are the institutional legal mechanisms and the international and national efforts to combat electronic financial crimes?* To answer this question, our research will address the following:

INTERNATIONAL AND NATIONAL CONFRONTATION OF ELECTRONIC FINANCIAL CRIMES

In order to encompass all aspects of effectively combating electronic crime, this research addresses the international and national confrontation of electronic financial crimes, the technical protection of information from electronic crimes, the international security agencies specialized in combating electronic financial crimes in the second section, the regional security institutions specialized in combating electronic financial crimes in the third section, and finally, the national institutions for combating electronic financial crimes under Algerian legislation in the fourth section.

Section One: Technical Protection of Information from Electronic Crimes

Computer programs are considered the first and most important informational and technical works that have received significant attention in terms of the need for recognition and protection. Software represents the intellectual component of the computer, without which its physical components would be useless. Given its importance, information security is regarded as a major challenge in the field of new information technologies. Due to the crucial role it occupies in modern societies, the field of information security has expanded to include systems, content, and services, with the aim of preventing, detecting, and minimizing attacks in these areas. The mission of information security is to ensure the integrity, confidentiality, availability, and traceability of data and its processing.

Information security can be defined as "the science that provides protection for information from the risks that threaten it, or the barrier that prevents any attack against it, through the necessary tools and measures designed to protect information from internal or external threats. It also includes the standards and procedures adopted to prevent unauthorized persons from accessing information through communications and to ensure the authenticity and integrity of these communications." [1]

The mechanisms for securing access to information networks and the protection systems used by electronic banks are presented in detail as follows:

Subsection One: Mechanisms for Securing Access to Information Networks

These include mechanisms through which information is protected from the risk of being disclosed or accessed by unauthorized persons. Therefore, if the owner of the information wishes to maintain its confidentiality, it is necessary to take the required steps to protect the secrecy of sensitive data and ensure that access is granted exclusively to authorized users or owners. In addition, appropriate measures must be taken to protect the information from unlawful use, such as deletion, alteration, or destruction.

Subsection Two: Protection Systems Used in Electronic Banks

Electronic banks seek to ensure technical protection for electronic payment operations and methods. They have developed systems that allow them to perform their functions with greater confidentiality and security, enabling verification of their clients' identities as legitimate account holders. Each user

is treated as a verified client whose access and actions are subject to proper regulatory controls, including systems such as secured electronic signatures, among others.

Section Two: International Security Agencies Concerned with Combating Electronic Financial Crimes

Facts have proven that no country, regardless of its power or level of development, can eliminate cross-border electronic crimes on its own. The security authorities of each country often come into conflict with the principles of respect for state sovereignty and judicial jurisdiction, which stand as obstacles to the detection, pursuit, and prosecution of such crimes beyond national borders. Therefore, the only way to achieve this goal is to create a space for cooperation and communication channels among national police agencies to coordinate their security efforts through the establishment of joint regional and international security bodies.

Subsection One: The International Criminal Police Organization (INTERPOL)

The International Criminal Police Organization (INTERPOL) is a permanent intergovernmental organization composed of 188 member states. It enjoys legal personality and full legal capacity to carry out its functions. The organization contributes to strengthening international police coordination, particularly in the absence of diplomatic relations between member states, while respecting human rights.

INTERPOL is composed of a set of bodies focusing on combating crime in general and international crime in particular, given the harm these crimes cause to humanity.

The International Criminal Police Organization (INTERPOL) is considered one of the oldest forms of police cooperation in combating crime. In 1904, a group of police specialists met and concluded an implicit agreement embodying the characteristics of international police cooperation. The following year, seven (7) Latin American countries agreed to exchange information about professional criminals operating within their territories. In 1914, a number of legal scholars and police officers representing fourteen (14) countries convened and approved the general principles of police cooperation. These principles focused on the methods to ensure rapid arrest and detention of criminals, harmonization of techniques in the criminal field, classification of criminal records at the international level, and standardization of extradition procedures. [2]

Subsection Two: The International Cyber Police Organization (CYBERPOL)

The International Cyber Police Organization (CYBERPOL) was established under Royal Decree No. 595.16/22 dated July 12, 2015, in the United Kingdom [3], and its headquarters was later transferred to Belgium pursuant to Article (01) of the organization's Basic Law, issued on July 2, 2015. This article defines the organization's components and its role in combating cybercrime. CYBERPOL operates under Belgian law governing international non-profit associations and organizations, as it is an international non-profit entity established to combat electronic crimes.[4]

CYBERPOL has developed an international strategy to prevent the growth of cybercrime, which includes a set of objectives and tasks distributed among its bodies. The organization's key missions and objectives include the following:

- **Establishing a program** that provides technical support to police agencies in member states, operating 24 hours a day. This program represents the first international mechanism for managing

cyber risks and is known as "**Cyber Watch**." It includes a digital database for monitoring international borders and detecting cyber threats within cyberspace.

- **Developing the necessary capacities, knowledge, and skills** to ensure effective responses to electronic crimes. In this regard, CYBERPOL has provided international educational and training programs in computing and cybersecurity to train its personnel and develop police expertise within member states. [5]
- **Monitoring websites, electronic addresses, and information networks** to detect harmful or illegal content that may affect the psychological, physical, or mental well-being of Internet users, in order to achieve a safer online environment. [6]
- **Promoting research and study in the field of cyber defense and security** to enhance the organization's capabilities as well as those of police agencies in other countries, with the aim of achieving a safer digital and electronic world. [7]

Section Three: Regional Institutions Specialized in Combating Electronic Financial Crimes

Several regional institutions have been established to combat crime as a result of the joint efforts of countries that often share geographical proximity, political borders, and common threats posed by transnational crimes such as electronic crime. Examples include the *Asian Police* ***(Asianpol)*** for Asian countries, the *American Police* ***(Ameropol)*** for the Americas, the *European Police* ***(Europol)*** and *Eurojust* for European countries, and the *African Union Mechanism for Police Cooperation* ***(Afripol)*** for African states, whose headquarters is located in Algiers, Algeria.

All of these are strong institutional mechanisms created to combat this criminal phenomenon and facilitate the arrest of offenders. However, due to the multiplicity of these institutions, this study will focus on three of them.

Subsection One: African Mechanisms of Confrontation (AFRIPOL as a Regional Institution for Combating Cybercrime)

The 22nd African Regional Conference, held in September 2013 in the city of Oran, Algeria, marked the initial step toward the creation of AFRIPOL. During this event, the directors and inspectors general of police forces from the African Union member states adopted the idea of establishing a mechanism for African police cooperation. Following several subsequent meetings, the mechanism was officially established in Algiers on February 11, 2014, under the name **African Union Mechanism for Police Cooperation (AFRIPOL).**

The first General Assembly of AFRIPOL, held at the El Aurassi Hotel in Algiers on May 14–16, 2017, constituted its formal establishment. The statutes governing AFRIPOL had previously been approved by African heads of state and government during the 28th Ordinary Session of the African Union Summit held in Addis Ababa, Ethiopia, in January 2017. [8]

Objectives and Functions of AFRIPOL

In accordance with Articles (03) and (04) of the Statute of the African Union Mechanism for Police Cooperation, AFRIPOL seeks to achieve several goals and missions, including:

- Assisting police institutions in member states in establishing a framework for cooperation among police bodies at the national, regional, continental, and international levels.

- Developing the capacities of police agencies in member states through advanced training programs and the creation of African centers of excellence.
- Enhancing coordination with similar entities to prevent and combat crime.
- Promoting mutual technical assistance, sharing of expertise, and best practices among police institutions to improve their efficiency and effectiveness.
- Facilitating mutual legal assistance, particularly the extradition of criminals, by easing the exchange and sharing of information and intelligence to prevent, detect, and investigate crimes in coordination with other operational mechanisms, whether regional or international.

AFRIPOL also works to develop continental tools for crime prevention and to establish a coordinated African strategy for combating various forms of serious crimes, including cybercrime. [9]

Furthermore, one of the key recommendations of AFRIPOL's Second General Assembly, held in Algiers on October 15–16, 2018, was to support and accelerate the activation of the AFSYCOM communication system for all police forces in member states to facilitate information and document exchange and ensure the effective performance of AFRIPOL's duties, in addition to any other tasks that may be assigned by the African Union's policymaking bodies.

Subsection Two: European Mechanisms of Confrontation (EUROPOL and EUROJUST as Regional Mechanisms for Combating Cybercrime)

Two regional mechanisms have been established in Europe to combat cybercrime: **Europol and Eurojust. Both are key agencies at the European level for combating** serious crimes in general and electronic crimes in particular crimes that have imposed themselves on the international, regional, and national scenes, necessitating effective mechanisms to confront their growing threat.

The European Police Office (Europol) is one of these operational mechanisms that plays a major role in combating cybercrime. Through its specialized units, Europol supports member states in investigating organized crime and cyberattacks, coordinating international operations, and facilitating intelligence exchange across borders.

Eurojust, on the other hand, serves as the judicial cooperation unit of the European Union. It supports national judicial authorities in coordinating investigations and prosecutions in cases involving serious cross-border crimes, including cybercrimes, ensuring legal harmonization and facilitating the exchange of evidence and judicial assistance among EU member states.

Subsection Three: In the United States of America (The International Internet Police)

The International Internet Police, also known as the Internet Police, was established as a security organization in the United States in 1986 to receive complaints from Internet users, pursue electronic offenders and hackers, gather evidence against them, and bring them to justice.

Headquartered in the state of Ohio, this organization aims to protect websites from hacking attempts by computer thieves (hackers) for commercial purposes. It provides protection services to contracted websites in exchange for a fee. Whenever a protected website faces a hacking attempt, the system repels the attack. If repeated attempts are made by the same hacker, the organization freezes (paneed) the part of the network responsible for Internet connectivity, causing the computer system (Windows) to lose access to the Internet.

Among the most notable websites protected by this organization are online shopping platforms, the Federal Bureau of Investigation (FBI) website, the websites of Arab Ministries of Interior, and the official website of the FBI itself. [10]

Subsection Four: Arab Mechanisms of Confrontation

With regard to mechanisms for confronting information crimes and governmental efforts to combat crime at the Arab level, several offices and specialized bodies have been established within Arab countries to fight electronic crimes. Among them, the following examples can be mentioned:

First: The Office for Combating Computer and Information Network Crimes in Egypt

In 2002, the Egyptian Ministry of Interior established a specialized body under the name "Department for Combating Computer and Information Network Crimes", affiliated with the General Directorate of Information and Documentation, pursuant to Ministerial Decree No. 13507 of 2002.

The department's duties include monitoring and tracking crimes arising from technological developments and pursuing their perpetrators using the latest technical and technological systems. Legal procedures are formalized after the technical tracking process and the apprehension of the offender, whose actions are legally characterized in accordance with the Penal Code.

Second: The Arab Bureau of Criminal Police

To achieve the objectives of the Charter of the League of Arab States and in the spirit of cooperation to maintain security by suppressing international crime and combating criminal activity in all its forms through joint collaboration among the security authorities of member governments employing all practical, preventive, and defensive means an international organization was established within the framework of the League of Arab States under the name "The Arab International Organization for Social Defense Against Crime."

The purpose of this organization is to study the causes of crime and its prevention, address the treatment of offenders, and ensure mutual cooperation among criminal police forces in Arab countries, including combating narcotics.

The organization fulfills its objectives through a General Assembly, an Executive Council, and permanent offices such as the Office for Combating Crime, the Office of Criminal Police which is of particular relevance here and the Office for Narcotics Control. [11]

Section Four: Institutional National Efforts to Combat Electronic Financial Crimes in Algerian Legislation

At the national level, the responsibility for investigation and inquiry into crimes in general is entrusted to the Judicial Police. The Algerian Code of Criminal Procedure defines the persons assigned judicial police functions. According to Article (12/01) of the Code of Criminal Procedure[12], judicial police duties are performed by magistrates, officers, agents, and employees vested with certain judicial police powers. Article (15) of the same Code specifies those who hold the status of judicial police officers.

Articles (21) and (28) of the Code define the employees entrusted with specific judicial police duties. The law classifies these officers into two main categories:

- The first category has the authority to handle all types of crimes and is known as the Judicial Police with General Jurisdiction.
- The second category is competent to investigate specific crimes and is referred to as the Judicial Police with Special Jurisdiction.

With the emergence of new types of crimes, including electronic crimes, the Judicial Police have become unable to adequately confront such crimes due to limited expertise and insufficient technical knowledge. Because of this, and given the unique nature of electronic crimes, it became essential to train and qualify officers in the field of cybercrime investigation, strengthen their technical skills, and expand their operational capabilities to ensure an effective response and prevent such offenses. [13]

The Algerian legislator has established special institutions, departments, and units dedicated to combating electronic crime. At the national level, these include:

- The National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies;
- The Central Department for Combating Electronic Crime under the Directorate General of National Security;
- The National Institute of Criminal Evidence and Criminology under the National Gendarmerie.

In addition, the legislator has targeted the development of a national system for information security as part of a broader strategy to protect information systems and infrastructures, which have become indispensable in daily digital operations.

To this end, Algeria established specialized units for investigating and combating electronic crimes under the Directorate General of National Security, the General Command of the National Gendarmerie, and the Ministry of National Defense. For clarity, this section is divided into three subsections:

- Subsection One: Units under the Directorate General of National Security.
- Subsection Two: Units under the General Command of the National Gendarmerie.
- Subsection Three: Units affiliated with the Ministry of National Defense.

Subsection One: Units under the Directorate General of National Security

As part of implementing a high-level security policy to confront electronic crimes, the Directorate General of National Security (DGSN) undertook the modernization of its organizational structure and the establishment of specialized units dedicated to combating this type of crime. Four specialized departments were created under the following divisions:

- The Scientific and Technical Police Directorate;
- The Economic and Financial Crimes Directorate;
- The Criminal Affairs Directorate;
- The Research and Analysis Department.

The responsibility for combating electronic crimes was assigned to:

First: The Scientific and Technical Police Directorate

This department is responsible for conducting investigations through specialized units, most notably the Central Forensic Police Laboratory in Châteauneuf (Algiers) [14]. The laboratory consists of 15 divisions and ranks second in Africa and first in the Arab world among forensic police laboratories. Additional regional laboratories have been established in Constantine and Oran, as well as three others in Ouargla, Béchar, and Tamanrasset.[15]

These laboratories include several technical divisions specialized in investigating and analyzing electronic crimes and digital evidence. Each laboratory consists of two main sections:

- **The Scientific Division**, which handles the analysis of evidence related to biology, forensic medicine, chemistry, toxicology, arson, and explosives.
- **The Technical Division**, which investigates and analyzes forensic evidence from crimes involving weapons, forgery, and cybercrime, with each type of case handled in a separate section.

The regional forensic laboratories in Constantine and Oran each include a dedicated department for investigating electronic crimes known as the Digital Evidence and Technological Traces Department, established in 2004. Initially created as a small division, it was later promoted to a full department due to the rapid increase in cybercrime cases. The department includes three sub-sections:

- A section for exploiting digital evidence obtained from computers and networks.
- A section for analyzing evidence from mobile phones.
- A section for voice analysis.

This department is staffed by eight (08) investigators—four (04) of whom are official police officers holding the status of judicial police officers, and the remaining four are auxiliary agents. Each member holds a university degree in computer science and possesses knowledge of legal procedures. They regularly undergo technical and legal training sessions to stay updated on the latest developments in cybercrime investigation.

Through its divisions and laboratories, this department provides technical support to police services and judicial authorities in cyber investigations. Its members respond to requests from police units specializing in cybercrime and from public prosecutors or investigating judges, usually in the form of letters rogatory, to assist during crime scene investigations and the seizure of digital evidence. They perform technical analyses of digital data and electronic evidence using specialized programs and tools for data recovery and forensic examination. [16]

During the judicial investigation stage, the department's role is primarily that of an expert, preparing technical reports and submitting them to investigating judges or trial courts as evidence. According to statistical data, in 2014, the department handled around 250 cases, including an international commission request from INTERPOL involving two young men from Constantine who attacked the Kuwaiti Ministry of Foreign Affairs' information systems and engaged in online fraud targeting individuals in the United States. In the first quarter of 2015, the department investigated more than 60 cases of electronic crimes. [17]

In addition to these units, the Central Department for Combating Cybercrime was established under the Directorate General of National Security. Initially founded as a small division in 2011, it served as the nucleus for combating cybercrime. Later, in 2015, the General Director of National Security

issued a decision formally creating the Central Department for Combating Crimes Related to Information and Communication Technologies.

Second: The National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies

As part of the legal, security, and political reforms recently undertaken by Algeria particularly in the area of judicial reform aimed at strengthening the rule of law and combating electronic crime several legal instruments have been enacted, leading to the establishment of specialized bodies and institutions equipped with human, material, and technical resources to facilitate investigation and inquiry. Among these institutions is the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies.

This authority was created pursuant to Article (13) of Law No. 09-04, which sets out the special rules for the prevention and combating of crimes related to information and communication technologies. The Algerian legislator explicitly provided for the establishment of the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies. [18]

However, on October 8, 2015, Presidential Decree No. 15-261 [19] was issued, defining the composition, organization, and operating procedures of the authority.

Approximately four years later, the legislator issued another decree, Presidential Decree No. 19-172, concerning the composition, organization, and operation of the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies. This decree consisted of 25 articles, with Article (24) repealing Presidential Decree No. 15-261.[20]

About thirteen (13) months later, the legislator issued Presidential Decree No. 20-183, reorganizing the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies. This decree included 38 articles, and Article (37) repealed the previous Presidential Decree No. 19-172. [21]

2. Functions of the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies

Article (14) of Law No. 09-04, referred to above, defines the functions of the authority as follows: "The authority referred to in Article (13) above shall particularly be responsible for the following:

a. Promoting and coordinating the process of preventing and combating crimes related to information and communication technologies.
b. Assisting judicial authorities and judicial police services in their investigations concerning crimes related to information and communication technologies, including information gathering and the preparation of judicial expertise.
c. Exchanging information with its foreign counterparts in order to collect data useful for identifying and locating perpetrators of crimes related to information and communication technologies."

Subsequently, Presidential Decree No. 20-183, mentioned above, reaffirmed these functions in Article (4), specifying that several of the authority's duties remain the same as those set forth in Article (14) of Law No. 09-04. These functions are as follows:

1. To propose elements of the national strategy for the prevention and combating of crimes related to information and communication technologies.
2. To promote and coordinate preventive operations against such crimes.
3. To assist judicial authorities and judicial police services in combating crimes related to information and communication technologies, particularly through the collection and provision of information and the preparation of judicial expertise.
4. To ensure preventive monitoring of electronic communications to detect crimes related to terrorism, sabotage, and threats to state security.
5. To collect and record digital data and identify their sources and transmission paths for use in judicial proceedings.
6. To ensure the execution of mutual assistance requests from foreign countries and to promote international information exchange and cooperation within its field of competence.

Subsection Two: Units under the General Command of the National Gendarmerie

As one of the main security bodies responsible for preventing and controlling crime and maintaining public order and security, the National Gendarmerie has kept pace with the recent evolution of criminal activity worldwide. It has done so by providing advanced technical means and training specialized officers in the fight against cybercrime. To this end, the Gendarmerie has established a range of structures and specialized units dedicated to investigating and analyzing this type of crime, alongside departments that handle general criminal inquiries. These include scientific and technical centers, the Central Criminal Investigation Department, specialized training structures, and operational support and regional units.

In addition to these departments, and in order to combat electronic crime effectively, the National Gendarmerie has established several specialized units and centers at the central, regional, and local levels.

First: At the Central Level

Three main institutions have been established:

1. The National Institute of Forensic Evidence and Criminology

The National Institute of Forensic Evidence and Criminology is a public administrative institution created by Presidential Decree No. 04-432 of December 29, 2004 [22], located in Boushawi, Algiers. It was established as part of the modernization of the National Gendarmerie sector.

The Institute consists of eleven (11) specialized divisions in various fields, all aimed at conducting expert analyses, providing technical assistance, and offering training and education. Among these divisions is the Information and Electronics Division, which is tasked with analyzing digital evidence obtained from electronic crimes. This division is organized into three laboratories, depending on the type of data or evidence being analyzed.

2. The National Center for Combating Cybercrime

This center was created as part of the National Gendarmerie's strategy to anticipate and swiftly respond to the rise of cybercrime, recognizing that digital technology has become a key facilitator

of modern criminal activity. Established in Algiers in 2004, the center includes several operational units responsible for investigating and analyzing cybercrimes:

- **The Surveillance and Analysis Unit (Unité de veille et d'analyse):**

  This unit continuously analyzes stored information and monitors open or circulating data across the Internet 24 hours a day. It ensures general oversight of informational content and safeguards data integrity.

- **The Assistance and Incident Response Cell (Cellule d'assistance et de réponse aux incidents informatiques):**

  This cell is responsible for preventing digital security risks and providing support to citizens, institutions, and public bodies in overcoming cyberattacks or electronic crimes.

- **The Central Coordination and Cybercrime Unit (Unité centrale de coordination et de lutte contre la cybercriminalité):**

  This unit supervises several **regional and local branches** located within provincial groups of the Gendarmerie. These local cybercrime units operate in coordination with the central unit, exchanging information and technical expertise related to investigations and digital evidence analysis.

3. The Center for the Prevention of Computer and Information Crimes

The Center for the Prevention of Computer and Information Crimes serves as a national contact point supporting cybercrime investigations and digital crime detection efforts. It is a technical body operating under the supervision of the Directorate of Public Security and Operations of the National Gendarmerie. Established in Algiers (Bir Mourad Raïs) in 2015, the center performs the following functions:

- Monitoring electronic communications within the limits permitted by law for the benefit of Gendarmerie units and judicial authorities.
- Assisting regional Gendarmerie units in investigating crimes related to information and communication technologies through Internet and digital device analysis.
- Participating in cyber investigations by infiltrating online networks on behalf of Gendarmerie services and judicial authorities.
- Ensuring continuous surveillance of the Internet network to detect and prevent online criminal activity. [23]

The center is responsible for investigating all types of crimes, including those linked to information and communication technologies. [24]

Second: At the Regional Level

Regional departments of the National Gendarmerie are responsible for coordinating between various judicial police units and providing logistical and technical support for investigations into electronic crimes. The Gendarmerie plays a key role in combating cybercrime due to its extensive territorial presence across Algeria, equipped with advanced tools and highly trained personnel capable of handling complex and serious offenses of this nature.

Third: At the Local Level

At the local level, the National Gendarmerie operates several specialized sub-units with extensive competence and expertise in investigating electronic crimes. These teams conduct complex investigations and play a crucial role in supporting regional research and inquiry operations.

These specialized units were reorganized on July 21, 2004, under Instruction No. 223-04 issued by the National Gendarmerie Command, in response to the growing complexity of observed crimes. A specialized cell for combating crimes related to information and communication technologies was created within seventeen (17) provincial groups, ensuring an effective national response to this form of crime. [25]

Subsection Three: Bodies under the Ministry of National Defense

Recently, Algeria decided to establish a National System for the Security of Information Systems, which constitutes the state's primary instrument for ensuring information security. This initiative was formalized through the Presidential Decree[26] establishing the National System for the Security of Information Systems, signed by the President of the Republic.

This system represents the organizational framework responsible for preparing, approving, and supervising the implementation of the national strategy for information systems security. It is tasked with conducting investigations in the event of cyberattacks, assessing and collecting data, providing advice to public institutions, and carrying out other missions related to the cybersecurity of state entities.

According to Article (3) of Presidential Decree No. 20-05, the system includes a National Council for the Security of Information Systems, which is responsible for drafting, approving, and guiding the national strategy. To carry out its duties, the council relies on structures operating under the authority of the Ministry of National Defense.

The system also includes a department called the Agency for the Security of Information Systems, which is responsible for coordinating the implementation of the national cybersecurity strategy. The following provides details on the composition and missions of these two entities:

First: The National Council for the Security of Information Systems

The National Council for the Security of Information Systems was established following the model of the electronic certification bodies created under Law No. 15-04 relating to electronic signatures and certification.

This council serves as a strategic and supervisory body that develops, approves, and oversees the national policy for information systems security. Its mission includes setting the overall orientation of Algeria's cybersecurity framework, ensuring the coherence of national initiatives, and providing coordination among the various institutional stakeholders involved in cybersecurity under the supervision of the Ministry of National Defense.

Second: The Agency for the Security of Information Systems

According to Article (17) of Presidential Decree No. 20-05, the Agency for the Security of Information Systems is a public administrative institution endowed with legal personality and financial autonomy, with its headquarters located in Algiers.

As provided in Article (18) of the same decree, the agency is entrusted with a set of specific tasks, which include:

- **Preparing the elements of the national strategy** for the security of information systems and submitting them to the Council for approval.
- **Coordinating the implementation** of the national strategy for the security of information systems as defined by the Council.
- **Proposing accreditation procedures** for service providers specializing in auditing information systems security.
- **Conducting digital investigations** in cases of cyberattacks or cybersecurity incidents targeting national institutions.

Through these bodies the Council and the Agency the Algerian state aims to build a comprehensive and integrated national cybersecurity framework capable of protecting critical infrastructures, supporting investigative efforts in the face of cyber threats, and strengthening the digital resilience of public and governmental entities.

CONCLUSION

We have reached a set of findings regarding the topic "Electronic Financial Crimes: A Comparative Study", summarized as follows:

First: Findings

- The crimes under study are characterized by their extreme seriousness due to their international nature, as they have become transnational crimes affecting the interests of more than one country.
- Electronic crime occurs in an environment completely different from that of traditional crime. It takes place outside the tangible physical realm, with its elements situated in the environment of computers and the Internet. This makes matters more complicated for the authorities responsible for investigation and inquiry, as electronic pulses flowing through the information system are invisible, allowing the perpetrator to easily erase evidence. Traditional inspection methods are therefore ineffective in proving this type of crime due to its distinctive nature compared to conventional crimes.
- Detecting and collecting evidence in electronic crimes is extremely difficult because the evidence is invisible and cannot be easily retrieved. The problem also lies in the fact that personnel in the competent authorities and investigation offices have the capability to conceal such evidence effectively.
- Information technology tools and networks represented by computers and the Internet are among the most important means of committing electronic crimes. However, they are not the only means, as such crimes can also be committed through other tools such as mobile phones or electronic tablets.
- The significant technological developments that led to the emergence of electronic banking, electronic money transfers, the use of magnetic credit cards, and ATMs have created fertile ground for crimes of theft, fraud, electronic deception, and money laundering. Consequently, some countries have hastened to enact laws regulating this type of electronic transaction.
- Many countries have issued specific measures, separate from their penal codes, to combat electronic financial crimes. These legislations include criminal penalties and aggravated

circumstances to deter offenders, in addition to special provisions criminalizing attacks targeting financial information stored in information systems.

- Electronic financial crimes are international crimes committed in one country but producing effects in another. Therefore, the available legal mechanisms within each country are insufficient to confront them. This has driven many countries to activate international measures to mitigate their negative effects, such as signing international conventions, holding conferences and symposiums against such crimes, adopting countermeasures included in official United Nations documents, strengthening security and judicial cooperation among all countries, and activating extradition systems to prevent cybercriminals from escaping punishment by fleeing abroad.

Based on these findings, we conclude that criminal legislation has made significant progress in addressing and understanding this type of crime. The Algerian legislator, in particular, has made great efforts to adapt both its substantive and procedural criminal policies to the specific and technical nature of electronic crime. However, there remain some shortcomings in several aspects. In light of this, we propose the following recommendations to address the main issues:

- Countries that have not yet enacted substantive and procedural criminal laws specific to electronic crimes such as many Arab states must accelerate the amendment and rationalization of their existing laws to ensure their applicability to such crimes, thereby addressing legislative deficiencies and closing legal loopholes that cybercriminals may exploit to escape prosecution and punishment.
- The Algerian legislator should expedite the adoption of the draft law on electronic crimes to curb financial attacks targeting information stored within information systems. We propose that the law be divided into four sections: the first devoted to general forms of electronic crimes, the second to crimes against persons, the third to electronic crimes against property, and the fourth to crimes targeting the security and safety of the state and its institutions.
- More conferences and scientific symposia should be organized on electronic financial crimes to raise awareness about their risks, explain their various methods of commission, and present the most recent preventive and legislative solutions adopted by comparative legislations particularly in developed countries to benefit from their experiences in combating such crimes.
- Broader powers should be granted to the National Authority for the Prevention of Crime Related to Information and Communication Technologies.
- The provisions of the Arab Convention on Combating Information Technology Crimes should be activated, particularly those related to judicial assistance and the extradition system, to enhance security and judicial cooperation.
- Awareness and digital culture should be promoted by activating the role of the media in spreading preventive awareness about electronic crimes especially financial onesand by engaging civil society through seminars, forums, and awareness days highlighting the dangers of this type of crime.

FOOTNOTES:

[1] Interpol website: https://ar.wikipedia.org/wiki/

[2] Hicham Bachir, The International Mechanisms for Combating Cybercrime, International Center for Strategic and Future Studies, No. 90, Year 8, June 2012, p. 21.

[3] Royal Decree° WL 22/16.595, Dated 02 July 2015, State Gazette n° 635.897.257.

[4] Hayti Fatima, Investigation Procedures in Cybercrimes: A Comparative Study, op. cit., p. 150.

[5] Official website of Cyberpol: https://www.cyberpol.info/ (Accessed on October 18, 2023, at 00:02).

[6] Hayti Fatima, Investigation Procedures in Cybercrimes: A Comparative Study, op. cit., p. 155.

[7] Article (02) of the Basic Law of the Organization.

[8] Chantir Khadra, Legal Mechanisms for Combating Cybercrime (A Comparative Study), op. cit., p. 259.

[9] Article (03) of the Statute of the African Union Mechanism for Police Cooperation mentioned above.

[10] Published on the website https://ar.wikipedia.org/wiki/ (Accessed on November 20, 2023, at 19:20).

[11] Article (03), paragraph (a) of the Convention of the Arab International Organization for Social Defense against Crime, held on November 3, 1977.

[12] Article (12) of Law No. 06-22 of December 20, 2006, amending and supplementing Ordinance No. 66-155 containing the Code of Criminal Procedure, Official Gazette No. 84, dated December 24, 2006, states: "The judicial police shall consist of judges, officers, agents, and employees specified in this section.

The judicial police within the jurisdiction of each Court of Appeal shall operate under the supervision of the Public Prosecutor, and the Public Prosecutor of the Republic shall manage it at the level of each court, under the oversight of the Indictment Chamber.
The judicial police are entrusted with the task of investigating and inquiring into crimes provided for in the Penal Code, collecting evidence, and searching for perpetrators, as long as no judicial investigation has yet begun.
The Public Prosecutor determines the general directives necessary for the judicial police to implement criminal policy within the jurisdiction of the Court of Appeal."

[13] Hayti Fatima, Investigation Procedures in Cybercrimes: A Comparative Study, op. cit., p. 115.

[14] It was inaugurated on July 22, 1999, comprising about 170 specialists and 500 crime scene technicians distributed across the capital's districts, in addition to regional laboratories in Oran and Constantine. All these laboratories are equipped with the latest advanced global technologies, and there are future projects to establish additional laboratories in Tamanrasset, Ouargla, and Béchar.

[15] The first laboratory established in the Arab countries was in Egypt in 1957, followed by Iraq, Jordan, Saudi Arabia, Kuwait, and the United Arab Emirates. In Algeria, the first scientific police laboratory was established on July 22, 1962, under the National Security, conducting analyses of physical evidence from crimes examined by the judicial police of the National Security or the National Gendarmerie.

[16] Hayti Fatima, Investigation Procedures in Cybercrimes: A Comparative Study, op. cit., p. 117.

[17] Rabii Hussein, Mechanisms of Investigation and Inquiry in Information Crimes, op. cit., p. 181.

[18] Article (13) stipulates that: "A National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies shall be established, its composition, organization, and mode of operation shall be determined by regulation."

[19] Presidential Decree No. 15-261 dated 24 Dhu al-Hijjah 1436, corresponding to October 8, 2015, determining the composition, organization, and operating procedures of the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies, published in the Official Gazette No. 53, dated October 8, 2015, p. 16 (repealed).

[20] Article (24) of Presidential Decree No. 19-172, which defines the composition, organization, and operating procedures of the National Authority for the Prevention and Combating of Information and Communication Technology Crimes, stipulates that: "All provisions contrary to this decree are repealed, particularly those of Presidential Decree No. 15-261 dated 24 Dhu al-Hijjah 1436, corresponding to October 8, 2015, which defined the composition, organization, and operating procedures of the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies."

[21] Article (37) of Presidential Decree No. 20-183 dated 21 Dhu al-Qi'dah 1441, corresponding to July 13, 2020, which reorganized the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies, published in the Official Gazette dated June 18, 2020, provides that: "All provisions contrary to this decree are repealed, particularly those of Presidential Decree No. 19-172 dated 3 Shawwal 1440, corresponding to June 6, 2019, which defined the composition, organization, and operating procedures of the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies."

[22] Presidential Decree No. 04-432 dated December 29, 2004, establishing the National Institute for Research in Criminal Investigation Science, Official Gazette No. 84, dated December 29, 2004, p. 24.

[23] Rabii Hussein, Mechanisms of Investigation and Inquiry in Information Crimes, op. cit., p. 185.

[24] Rabii Hussein, ibid., p. 183.

[25] Rabii Hussein, ibid., pp. 186–187.

[26] Presidential Decree No. 20-05 dated 24 Jumada al-Awwal 1441, corresponding to January 20, 2020, concerning the establishment of a National System for the Security of Information Systems, Official Gazette No. 04, dated January 26, 2020, p. 05.