

**Crimes Associated with ICT and Communication Technology: Preventive Measures
(In Accordance with Law No. 09-04 on the Prevention and Suppression of Offenses
in the Digital Domain)**

الجرائم المتصلة بتكنولوجيا الاعلام والاتصال وآليات الوقاية منها

وفقا للقانون رقم 04-09 المتعلق الوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها



Boudjelal fatma zohra ^{1*}

¹ Laboratory of Comparative Private Law, Faculty of Law and Political
Science, University of Hassiba Ben Bouali, Chlef, Algeria

f.boudjelal@univ-chlef.dz

Date of transmission: 28/03/2025 date of acceptance: 05/05/2025 date of publication: 01/06/2025

Abstract:

Recent decades have witnessed significant progress in information and communication technologies, which have greatly eased everyday tasks and bolstered the efficiency of many sectors. These technological advances have woven themselves into the fabric of daily life—ranging from bill payments and personal communication to both traditional and remote educational and work activities. They have also optimized administrative and commercial transactions online with notable rapidity and precision. This swift evolution has fueled social progress and spurred digital transformation across various fields, thereby enhancing service quality

Yet, alongside these benefits, technology's evolution has introduced a host of new challenges and hazards. The ever-growing dependence on these tools, paired with their widespread application, has made it almost unfeasible to completely control or restrict their use. As a result, novel types of offenses have surfaced—offenses that are inherently digital and often employ electronic means in their execution.

In light of these challenges, there is an urgent need to implement legal frameworks that address the distinctive traits of these offenses and minimize their impact. In response, the Algerian legislature enacted Law No. 09-04, which primarily emphasizes proactive measures over mere punitive responses.

key words: Cybercrimes; Digital Crimes; Information and Communication Technology; Combating Cybercrime

الملخص:

شهدت العقود الأخيرة تقدماً كبيراً في تكنولوجيا المعلومات والاتصالات، مما سهل المهام اليومية وزاد من كفاءة العديد من القطاعات. هذه التقدّمات التكنولوجية أصبحت جزءاً لا يتجزأ من الحياة اليومية من دفع للفواتير والتواصل الشخصي، وصولاً إلى التعليم والتعلم عن بعد، كما ساهمت في تحسين المعاملات الإدارية والتجارية بأن أصبحت تتم بسرعة ودقة، وقد أدى هذا التطور السريع إلى تحفيز التقدم الاجتماعي ودفع هذا التحول الرقمي في مختلف المجالات إلى تعزيز جودة الخدمات.

غير أنه وإلى جانب هذه الفوائد، تسببت تطورات التكنولوجيا مجموعة من التحديات والمخاطر الجديدة. إن الاعتماد المتزايد على هذه الأدوات، جنباً إلى جنب مع انتشار استخدامها، جعل من شبه المستحيل التحكم الكامل أو تقييد استخدامها. ونتيجة لذلك، ظهرت أنواع جديدة من الجرائم الجرائم التي هي بطبيعتها رقمية وغالباً ما تستخدم الوسائل الإلكترونية في تنفيذها.

في ضوء هذه التحديات، هناك حاجة ملحة لتنفيذ أطر قانونية تتناول الخصائص المميزة لهذه الجرائم وتقلل من تأثيرها. استجابة لذلك، أقرّ المشرع الجزائري القانون رقم 04-09، الذي يركز بشكل أساسي على التدابير الاستباقية بدلاً من الردود العقابية فقط.

الكلمات المفتاحية: الجرائم الإلكترونية، الجرائم الرقمية، تكنولوجيا الإعلام والاتصال، مكافحة الجريمة الإلكترونية.

* Corresponding Author

Introduction:

The fast-paced development of digital technologies has profoundly transformed everyday life and continues to shape numerous sectors. This technological progress now underpins a variety of daily interactions—from paying bills and maintaining communication to engaging in both conventional and online educational and work-related activities. Additionally, it has facilitated the rapid and effective processing of commercial and administrative tasks online, thus propelling societal advancement and widespread digital adoption. The emergence of artificial intelligence further refines service delivery and is anticipated to drive even greater changes, with some viewing it as the foremost revolution in information technology.

However, these benefits come with significant drawbacks. The increased reliance on technology, along with its expansive reach, has made oversight and regulation a growing challenge. This situation has paved the way for a spectrum

***Crimes Associated with ICT and Communication Technology: Preventive Measures
(In Accordance with Law No. 09-04 on the Prevention and Suppression of Offenses in the
Digital Domain)***

of issues, notably cyber offenses. Such crimes, executed using contemporary digital tools, are not only serious but also alarmingly straightforward to commit. They generally involve breaches of electronic security systems to access confidential or restricted data for either material or immaterial gains. While unauthorized access is often attributed to “novice hackers,” those who alter or manipulate information systems with harmful intent are recognized as seasoned cybercriminals.

In response to these emerging threats, the Algerian legislator—mirroring trends in other legal systems—has updated the Penal Code via Law No. 04-15 to introduce specific provisions on “Offenses Against Automated Data Processing Systems” (Articles 394 bis to 394 bis 7). Alongside this, Algeria adopted a specialized legal instrument, Law No. 09-04, which is dedicated to preventing and suppressing digital crimes. This law supplements the Penal Code by offering a legal framework adapted to the unique aspects of cyber offenses, integrating procedural safeguards to counter cybercrime and establishing preventive measures to mitigate such risks. Addressing cybercrime is not solely a legal concern; it also touches on social and economic domains. This holistic approach is further reinforced by regulatory measures such as Presidential Decree No. 15-261 of October 8, 2015—later amended by Presidential Decree No. 20-282—as well as Law No. 18-07 for data protection¹ and Ordinance No. 21-11 of August 25, 2021, which established a dedicated judicial branch for cybercrime investigations.

Before discussing the criminalization and prevention mechanisms for these acts, it is essential to clarify the notion of cybercrime. Although Law No. 04-15 amends the Penal Code without providing a precise definition—referring instead to “offenses against automated data processing systems”—scholars have defined cybercrime as “a series of illegal acts conducted via electronic devices and networks intended to harm individuals or institutions by unlawfully accessing their information systems.” Alternatively, it is described as “a criminal act where a computer is the main instrument used in the commission.” Essentially, cybercrime involves exploiting modern digital devices, such as computers and mobile phones, to perpetrate illicit activities that imperil public security.

¹ -Law No. 18-07, dated June 10, 2018, concerning the protection of natural persons in the field of personal data, Official Gazette, No. 34, dated June 10, 2018.

Subsequently, the Algerian legislature clarified its stance with an explicit definition in Law No. 09-04. In Article 2, this law specifies cybercrimes as “offenses against automated data processing systems as provided in the Penal Code, as well as any offense committed or facilitated via an electronic communication system or network.”

The purpose of this study is to explore the range of cyber offenses tackled by the Algerian legislator under Law No. 09-04 and to evaluate the preventive measures incorporated within the updated legal framework. The central research question is:

How has the Algerian legislature addressed cyber offenses under Law No. 09-04 on the Prevention and Suppression of Digital Crimes?

To answer this question, the study is divided into two primary chapters. The first chapter categorizes different cyber offenses and identifies the authorities responsible for their investigation and prosecution. It includes two sections: the first details the various forms of cybercrime, and the second outlines the entities involved in detecting and enforcing these laws. The second chapter focuses on the procedural techniques for gathering electronic evidence and assessing its legal validity. This chapter is similarly segmented into two parts: the first discusses the investigative procedures for collecting digital evidence, and the second examines its admissibility in court. An analytical methodology is used to critically assess relevant legal texts, complemented by a descriptive approach to explain various doctrinal perspectives on the subject.

Chapter One: Types of Cyber Offenses and the Investigative Authorities

The concept of “cybercrime” encompasses a broad range of offenses, as identified by the Budapest Convention¹ and further refined by Algerian legislation. These legal provisions not only classify various types of cyber offenses but also designate the agencies responsible for their investigation and enforcement. Accordingly, this chapter is divided into two sections: the first

¹ -The Budapest Convention on Cybercrime, stemming from the European Council meeting in Budapest, Hungary, under number 185, dated November 23, 2001, established a new classification for cybercrime as follows :

- **Crimes targeting information elements (confidentiality, integrity, and availability of data and systems):** Unauthorized access, Unauthorized interception, Data interference, System interference.
- **Computer-related crimes:** Computer-related fraud, Computer-related forgery.
- **Crimes related to content and systems, including offenses related to child pornography.**
- **Crimes related to violations of copyright and related rights.**

examines the distinct forms of cybercrime, while the second describes the agencies and supporting bodies tasked with investigating these offenses.

Section One: Varieties of Cyber Offenses

Under Law No. 09-04¹, the Algerian legislature classified cyber offenses into two broad categories. The first category involves crimes that target automated data processing systems, while the second encompasses offenses facilitated through broader information systems. The former category is detailed in the Penal Code (Articles 394 bis to 394 bis 8), which criminalizes various forms of intrusion and attacks on such systems. The latter, due to its varied nature, is addressed across several legal instruments.

Firstly: Unauthorized Entry and Unlawful Occupancy of Automated Systems

Outlined in Article 394 bis of the Penal Code, this offense involves unlawfully entering or remaining within an automated system or a segment of it². Its material element is defined by the act of access or occupancy, while the mental element comprises the deliberate intent to commit the offense, done with full awareness of its illegality. Penalties range from six months to two years of imprisonment and fines between 60,000 and 200,000 DZD³, with harsher sentences applied if the act results in data deletion, alteration, or if the system's integrity is compromised. the penalty increases to imprisonment for one year to three years, along with a fine ranging from 100,000 to 300,000 DZD⁴.

Secondly : Unauthorized Alteration of Automated Systems

Addressed in Article 394 bis 1 of the Penal Code, this offense involves the fraudulent insertion, removal, or modification of data within an automated system. Similar to other cyber offenses, both the physical act and the conscious intent are key components. The punishment for this violation may include imprisonment from six months to three years and fines ranging from 50,000 to 400,000 DZD.

¹ - Article 2 of Law No. 09/04, dated 05/08/2009, containing the specific rules for the prevention and combating of crimes related to information and communication technologies, Official Gazette, Issue No. 47, published on 16/08/2009.

² - Batehi Nesma, "The Crime of Unauthorized Access or Stay in an Information System," Journal of Legal and Political Jurisprudence, Volume 01, No 1, p. 79.

³ -Article 394 bis of Law No. 24-06, dated April 28, 2024, amending and supplementing Ordinance No. 66-156, dated June 8, 1966, concerning the Penal Code.

⁴ -Article 394 bis, Paragraph 3, of the aforementioned Penal Code.

Thirdly: Handling Illicitly Obtained Data

Detailed in Article 394 bis 2, this category covers several criminal actions, such as:

A) Utilizing Data to Facilitate a Crime:

1. Design: The initial phase involves preparing data or developing software tools (such as viruses, malware, or hacking utilities) intended for cyberattacks.
2. Research: Involves analyzing methods used to craft these digital tools.
3. Aggregation: The process of collecting data fragments that may later be used in cyber offenses.
4. Provision: Making such data accessible to enable crime commission.
5. Dissemination: Circulating or publishing this data online.
6. Trafficking: The illegal exchange or sale of confidential data for monetary or other benefits.

B) Dealing with Data Derived from Criminal Activity:

Includes possessing or disseminating data obtained through illegal means. The corresponding penalty for these offenses is one year to three years of imprisonment and fines between 500,000 and 2,000,000 DZD. The law further increases the severity of penalties if the crimes target national defense or public institutions. Additionally, Articles 394 bis 4 and 394 bis 6 establish that legal entities found guilty will face fines up to five times the maximum imposed on individuals, and accomplices are subject to equivalent penalties. Article 394 bis 7 even authorizes the confiscation of tools, software, and website closures associated with the offense.

Section Two: Investigative Authorities and Support Structures

This section outlines the units within the National Police and National Gendarmerie that handle cybercrime investigations, along with the auxiliary bodies that support judicial operations.

Firstly: Cybercrime Investigation Units

A)- National Police Units:

The task of investigating cyber offenses has been delegated to the National Scientific and Technical Police Directorate, which includes:

1. The Central Laboratory of Scientific Police in Algiers.
2. Regional Scientific Police Laboratories in Constantine and Oran.
3. Additional laboratories under development in Ouargla, Béchar, and Tamanrasset, as well as dedicated cybercrime units integrated within the Judicial Police across Algeria's central, western, and eastern regions.

B)-National Gendarmerie Units:

A National Center for Combating Cyber Offenses has been established under the National Gendarmerie, with specialized training provided to its members. This structure includes:

1. Central Directorate of Public Security and Intelligence: Coordinating regional units and the National Technical and Scientific Center for cyber investigations.
2. Central Criminal Investigations Division: A nationwide unit focused on cyber offense investigations.
3. National Institute of Forensic Science and Criminology: Established in 2004 to support these efforts.
4. Center for the Prevention of Cybercrime: Launched in 2008 to streamline cyber offense prevention and investigation at both regional and local levels.

Secondly: Judicial and Technical Support Bodies

A) National Authority for Preventing and Combating Cyber Offenses:

Formed under Law No. 09-04 and governed by Presidential Decree No. 183-20 (dated July 13, 2020), this independent administrative body operates under the President's supervision. Its mandate includes promoting international cooperation in judicial and security matters¹, coordinating preventive actions, and providing technical support to judicial bodies. Its organizational structure consists of:

1. A Guidance Council, chaired by the President, that meets biannually (with provisions for special sessions) and oversees strategic directives.
2. A General Directorate led by a Director General, responsible for daily operations and divided into departments such as Preventive Surveillance, Administration, Studies, Cooperation, and Technological Vigilance.

This Authority is also tasked with:

- Contributing to the national strategy against ICT-related crimes.

¹ - Souhila Bouzebra, "The National Authority for the Prevention of Crimes Related to Information and Communication Technology: Data Privacy and Electronic Crime Combat," Critical Journal of Law and Political Science, Volume 17, No 02, 2022, p. 565.

- Organizing and coordinating prevention campaigns¹.
- Aiding judicial bodies through technical and legal expertise².
- Monitoring electronic communications to preempt acts of terrorism or sabotage.
- Ensuring the collection and preservation of digital evidence.
- Facilitating international legal assistance and information exchange.
- Promoting training for investigators in digital crimes.
- Proposing legislative updates to better align the legal framework with technological progress³.

B) Service Providers:

As defined by Article 2(d)⁴ of Law No. 09-04, service providers are any public or private organizations offering communication services or handling data on behalf of users. According to Article 10, these providers must assist judicial investigations by collecting, recording, and preserving communication data in real time, as well as safeguarding stored information as stipulated by Article 11. They are also responsible for promptly removing content that breaches the law and implementing measures to restrict access to illegal data. Failure to meet these obligations can result in criminal penalties for both individuals and companies.

Chapter Two: Methods for Collecting Electronic Evidence and Its Judicial Significance

This chapter examines the evolving procedures for gathering digital evidence and its acceptance in judicial processes.

Section one: Investigative Methods for Digital Evidence

With the rapid expansion of automated systems, conventional approaches to evidence collection have had to evolve to meet the specific challenges of digital evidence. This section reviews traditional investigative methods and the modern adaptations needed for cyber offenses.

¹ -Fatiha Bouhrine, "Cybercrime in Algerian Legislation," Journal of Law and Human Sciences, Volume 14, No 04, 2021, p. 56.

² -Souhila Bouzebra, Op. cit., pp. 556-567.

³ -Souhila Bouzebra, Op. cit, p.571

⁴ - Presidential Decree No. 183-20, dated July 13, 2020, regarding the reorganization of the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies, Official Gazette No. 40, published on July 18, 2020.

Firstly: Conventional Evidence-Gathering Techniques

Traditional methods, including search and seizure, expert testimony, and on-site inspection, continue to be pivotal in criminal investigations but have been adapted to suit digital contexts.

A) Search:

Although not explicitly defined, a search is regarded as an essential procedure for uncovering evidence while balancing the risk of infringing on personal rights¹. The Algerian Constitution, notably Article 40, mandates that searches must adhere strictly to legal requirements and be performed only with judicial authorization. Law No. 09-04 (Article 5/1) allows judicial authorities to remotely access information systems to search for evidence, focusing on both physical hardware and the intangible digital content stored within².

B) Inspection:

Traditionally, inspection involves a detailed examination of a crime scene to identify relevant evidence and potential suspects. In the digital arena, inspection shifts focus to the virtual environment—analyzing the hardware, software, and data within computers and networks.

C) Expert Testimony:

Given the technical complexity of cybercrimes, expert witnesses play a crucial role. Specialists such as programmers, system analysts, engineers, computer operators, and IT administrators are often called upon to elucidate the technical aspects of the evidence. Law No. 09-04 encourages involving experts who possess in-depth knowledge of the systems under investigation³.

Secondly: Contemporary Methods for Digital Evidence Collection

Recognizing the unique challenges of cyber offenses, Algerian law now incorporates special procedural rules for evidence collection:

A) Infiltration:

As defined in Article 65 bis 12 of the Criminal Procedure Code (amended by Law 06-22), infiltration involves law enforcement officers covertly integrating into online environments—such as chat rooms or social media—

¹ -Khaled Mamdouh Ibrahim, *The Art of Criminal Investigation in Cybercrimes*, Dar Al-Fikr Al-Jami'i, Alexandria, 2010, p. 18.

² -Law No. 09-04, which includes the specific rules for the prevention and combating of crimes related to information and communication technologies, dated 05/08/2009, Official Gazette, issued on 16/08/2009, No. 47.

³ - Law No. 09-04, as previously mentioned

to monitor suspects. This method requires formal judicial authorization and must satisfy strict criteria regarding the specific crimes under investigation.

B) Electronic Surveillance:

Law No. 09-04, along with amendments to the Criminal Procedure Code, authorizes judicial officers to intercept electronic communications. This can include:

- 1- **Digital Communication Interception:** Using specialized software to monitor emails, text messages, and other online communications.
- 2- **Postal Communication Surveillance:** Extending these measures to traditional mail when applicable.
- 3- **Audio and Visual Recording:** Capturing sound and images using electronic devices, with strict judicial oversight, for cases involving threats to state security or public order.

C) Urgent Preservation of Digital Data:

In line with Article 16 of the Budapest Convention on Cybercrime (ratified by Algeria in 2001), service providers are compelled to immediately preserve electronic data that could serve as evidence in an investigation.

D) Data Seizure:

Law No. 09-04 also empowers authorities to seize digital data. This may involve either copying the relevant data onto secure storage¹ or blocking unauthorized access to ensure that evidence remains intact for judicial examination.

Section two: Judicial Assessment of Digital Evidence

Given the susceptibility of digital evidence to alteration or tampering, its judicial value is determined by a criminal judge's evaluation of its reliability and integrity.

Firstly: Judge's Evaluation:

Evidence is generally defined as the means by which a judge forms their conviction in order to arrive at the truth. Although Law No. 18-07 does not provide a specific definition of electronic evidence, However, it is legally defined as evidence derived from computer systems, existing in the form of magnetic or electrical impulses or fields. These can be

¹ -- Abd El-Sadik Sheik, "Prevention of Cybercrimes under Law No. 09-04 Containing Special Provisions for the Prevention of Crimes Related to Information and Communication Technologies," Ma'alim Journal of Legal and Political Studies, No 1, 2020, p. 200.

***Crimes Associated with ICT and Communication Technology: Preventive Measures
(In Accordance with Law No. 09-04 on the Prevention and Suppression of Offenses in the
Digital Domain)***

collected and analyzed using specialized software, applications, and devices to present information in various formats¹.

The Algerian legislator has subjected this type of evidence to the same principle that governs all other forms of evidence: the judge's personal conviction, as stipulated in Article 307 of the Criminal Procedure Code.

Secondly: Admissibility Standards:

The Algerian Legislator's Position on the Admissibility of Electronic Evidence

The duty of the criminal judge—whether an Investigating Judge, the Chamber of Charges, or a Criminal Court—is to assess evidence against the defendant. It is not sufficient to convict the accused solely based on circumstantial evidence; there must be sufficient proof in conjunction with other material evidence. Furthermore, the procedures for collecting evidence must adhere to legality, respecting the personal freedoms of the accused, who is presumed innocent until proven guilty.

Criminal evidence is anything that leads to the discovery of a crime, establishes proof of its occurrence, and confirms that the accused is indeed the perpetrator. Evidence is the legal means by which a judge reaches the truth and attributes the crime to the accused.

Legal doctrine has established two procedural systems in criminal evidence law: the restricted system and the free system. Algeria adopts the free system, similar to countries in the Latin legal tradition, such as France, Belgium, Jordan, and Syria. This system is reinforced by Article 212 of the Criminal Procedure Code, which states:

“Crimes can be proven by any method of proof unless the law stipulates otherwise. The judge may issue their decision based on their personal conviction, provided that the decision is only based on evidence presented during the hearings and discussed in the presence of the judge.”

Conclusion :

The analysis of Law No. 09-04 reveals that while the current legal framework has significantly advanced in addressing cyber offenses, rapid technological developments continue to challenge its efficacy. The evolving nature of digital

¹ -Mahmoud Sobhi Mohamed Mahmoud Zayed, The Admissibility of Electronic Evidence in Criminal Proof and the Judge's Authority in Its Evaluation, Banha Journal of Humanities, No 1, Part 2, Egypt, 2022, p. 30.

crimes poses persistent threats to national security, public safety, and economic stability. Consequently, the establishment of specialized judicial units—such as the one created under Ordinance No. 21-11 (August 25, 2021)—is a critical step forward.

Recommendations

- **Specialized Training:**

Enhance the training of experts, investigators, and judges in the technical aspects of cybercrime to ensure effective investigations.

- **Technical and Legal Guidelines:**

Develop comprehensive manuals that outline cyber offenses, detection methodologies, and evidence-handling procedures.

- **Inter-Agency Collaboration:**

Foster closer cooperation among different security agencies to share expertise and streamline evidence-gathering techniques.

- **Victim Reporting:**

Encourage victims to report cyber offenses and establish protocols for collaboration between legal authorities and IT experts.

- **Resource Allocation:**

Ensure that specialized centers combating cybercrime are adequately staffed and equipped with the necessary technological tools.

- **Educational Integration:**

Incorporate cybercrime awareness and digital literacy into educational curricula at various levels.

- **International Cooperation:**

Strengthen ties with international partners to address the borderless nature of cyber offenses effectively.

List of sources and references:

1- Conventions:

- **The Budapest Convention on Cybercrime**, stemming from the European Council meeting in Budapest, Hungary, under number 185, dated November 23, 2001,

2- Laws :

- **Law No 09-04**, dated 05/08/2009, containing the specific rules for the prevention and combating of crimes related to information and communication technologies, *Official Gazette*, Issue No. 47, published on 16/08/2009.

***Crimes Associated with ICT and Communication Technology: Preventive Measures
(In Accordance with Law No. 09-04 on the Prevention and Suppression of Offenses in the
Digital Domain)***

- **Law No. 18-07**, dated June 10, 2018, concerning the protection of natural persons in the field of personal data, Official Gazette, No. 34, dated June 10, 2018.
- **Law No. 24-06**, dated April 28, 2024, amending and supplementing Ordinance No. 66-156, dated June 8, 1966, concerning the Penal Code.
- **Presidential Decree No. 183-20**, dated July 13, 2020, regarding the reorganization of the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies, *Official Gazette* No. 40, published on July 18, 2020.

3- Books:

- **Khaled Mamdouh Ibrahim**, The Art of Criminal Investigation in Cybercrimes, Dar Al-Fikr Al-Jami'i, Alexandria, 2010.

4- Articles:

- **Abd El-Sadik Sheik**, "Prevention of Cybercrimes under Law No. 09-04 Containing Special Provisions for the Prevention of Crimes Related to Information and Communication Technologies," *Ma'alim Journal of Legal and Political Studies*, No 1, 2020.
- **Batehi Nesma**, "The Crime of Unauthorized Access or Stay in an Information System," *Journal of Legal and Political Jurisprudence*, Volume 01, No 1.
- **Fatiha Bouhrine**, "Cybercrime in Algerian Legislation," *Journal of Law and Human Sciences*, Volume 14, No 04, 2021.
- **Mahmoud Sobhi Mohamed Mahmoud Zayed**, The Admissibility of Electronic Evidence in Criminal Proof and the Judge's Authority in Its Evaluation, *Banha Journal of Humanities*, No 1, Part 2, Egypt, 2022.
- **Souhila Bouzebra**, "The National Authority for the Prevention of Crimes Related to Information and Communication Technology: Data Privacy and Electronic Crime Combat," *Critical Journal of Law and Political Science*, Volume 17, No 02, 2022.