

Mechanisms for Using Electronic Evidence in Algerian Criminal Law

آليات استخدام الدليل الالكتروني في القانون الجنائي الجزائري

Benderrah Ali Ibrahim¹,

¹ Aflou University Center (Algeria), a.benderrah@cu-aflou.edu.dz
Laboratory of Legal and Economic Studies - Aflou University Center

Received: 14/10 /2025

Accepted: 21/07 /2026

Published: September /2026

الملخص:

يحتل الدليل الالكتروني مكانة هامة في ميدان الاثبات الجنائي خاصة مع انتشار مختلف الجرائم ذات الطبيعة الجنائية الالكترونية، حيث عمدت مختلف القوانين الجنائية المقارنة إلى تحديد كفاءات توظيف هذا النوع من الأدلة خدمة لصالح التحقيقات الجنائية بما في ذلك المشرع الجزائري .

هذا التوظيف الذي جمع بين الجانب الموضوعي والاجرائي لاسيما من ناحية تحديد كفاءات استخدام الأجهزة البصرية الالكترونية اضافة إلى انشاء ما يعرف بالقطب الجزائري الوطني لمكافحة الجرائم المتصلة بتكنولوجيات الإعلام والاتصال من خلال قانون الاجراءات الجزائية.

الكلمات المفتاحية: الدليل الالكتروني - الحماية الجنائية - الأجهزة البصرية الالكترونية - كاميرات المراقبة - تكنولوجيات الإعلام والاتصال.

Abstract:

Electronic evidence has acquired a pivotal status within the domain of criminal proof, particularly in light of the proliferation of offences of an electronic and cyber-criminal nature. Comparative criminal legislations have endeavored to delineate the modalities for the admissibility and use of such evidence in the service of criminal investigations, a trend also embraced by the Algerian legislator. This regulatory framework integrates both substantive and procedural dimensions, notably with regard to the modalities governing the use of electronic optical devices, as well as through the establishment of the so-called National Criminal Division for Combating Offences Related to Information and Communication Technologies, introduced pursuant to the Algerian Code of Criminal Procedure.

KEY WORDS: electronic evidence – penal protection – optical surveillance devices – closed-circuit television (CCTV) – information and communication technologies (ICT).

1. Introduction

The advent of the computer, which succeeded the industrial revolution and the development of machinery, inaugurated a new era—globalization. This era has profoundly impacted all facets of human life, owing to the unprecedented scientific and technological advances and the novel forms they have imposed upon contemporary societies.

The challenges arising therefrom have not remained confined to traditional domains, but have extended into the realm of criminal proof with the emergence of cybercrime. Such offences have generated unprecedented modalities of criminal conduct, stemming from the misuse of technological means. Cyberattacks have targeted various information systems, adversely affecting the personal and financial interests of users of modern technologies as well as multinational corporations, thereby inflicting substantial economic losses.

This phenomenon is attributable to the misuse of emerging technologies, particularly information technology, which has played a decisive role in economic, social, industrial, and administrative transformations, culminating in what is now termed “technocrime.”¹

These developments have profoundly influenced mechanisms of criminal proof. Legal systems are now confronted with electronic evidence, which differs fundamentally from traditional forms of criminal evidence and is increasingly recognized as a form of compelling proof. The resort to such evidence has thus become an inevitability to safeguard societal security. Consequently, electronic evidence has been incorporated into the field of criminal proof as an advanced scientific method of ascertaining the truth, while ensuring respect for the fundamental rights and freedoms of the accused as enshrined in law.

We thus raise the following main research question:

What are the mechanisms through which electronic evidence is employed to ensure criminal protection under the Algerian law?

This overarching issue gives rise to a set of subsidiary questions:

- What are the general systems of criminal proof, and which system has been adopted by the Algerian legislator?
- In what manner is electronic evidence utilized within the framework of criminal proof, and how has it been regulated under Algerian law?
- What procedural mechanisms has the Algerian legislator established to facilitate the admissibility and use of electronic evidence?

In addressing this question, the study pursues the following aims and objectives:

1. To examine the general systems of criminal proof and to determine the specific model adopted by the Algerian legislator.

2. To analyze the legal framework governing the use of electronic evidence within the context of criminal proof, with a focus on its substantive and procedural dimensions.
3. To identify and evaluate the procedural mechanisms introduced by the Algerian legislator for the admissibility, collection, and use of electronic evidence in criminal proceedings.

Through these objectives, the study seeks to clarify the extent to which electronic evidence contributes to the realization of criminal protection, while maintaining a balance between the efficiency of criminal investigations and the safeguarding of fundamental rights and freedoms.

The analytical method adopted in this study serves to elucidate the foundations upon which the Algerian legislator has relied in regulating the use of electronic evidence. This method is equally useful for examining the causes, trends, and dimensions of various social phenomena—among which electronic evidence stands as a phenomenon warranting in-depth legal inquiry.

The study further employs the techniques of correlation, interpretation, and classification, which constitute indispensable tools for drawing coherent legal conclusions. On this basis, the hypotheses underlying the present research, to be tested either affirmatively or negatively, are as follows:

1. A study of the concept of electronic evidence necessarily entails an examination of its primary point of reference, namely the system of criminal proof.
2. The treatment of electronic evidence within the framework of general provisions inevitably raises the question of evidentiary rules and their treatment by the Algerian legislator.
3. A comprehensive study of electronic evidence requires an analysis of both its substantive modalities of use and its procedural regulation.

The principal objective of this study is to determine how the Algerian legislator has addressed the issue of electronic evidence, particularly within the field of criminal law. To this end, the research undertakes a review of the relevant legislative and regulatory texts governing this matter, followed by an analysis of their procedural application.

2. Systems and Rules of Criminal Evidence

In this section, we shall examine the systems of criminal proof and the rules governing such systems.

2.1. Systems of Criminal Evidence

Comparative legal systems have historically recognized three principal models of criminal proof: the restricted (or statutory) system, the absolute (or free) system, and the mixed system. Each of these reflects a distinct conception of the judge's role in the evidentiary process and the extent of legislative control over admissible proof.

2.2.The Restricted (Statutory) System

Also referred to as the legal proof system, this model is characterized by the legislature's broad prerogative to predetermine the admissible means of proof available to the judge². The legislature may prescribe the probative force of certain forms of evidence and, in some cases, condition the judge's decision upon the production of specific evidence depending on the nature of the offence and the corresponding penalty. Under this system, the judge is strictly bound by the provisions of criminal law. His or her discretion is curtailed, and the decision is limited to verifying the availability of the legally prescribed evidence without recourse to personal conviction or inner belief.

2.3.The Absolute (Free) System

In contrast, the free proof system releases both the parties and the judge from legislative constraints in matters of evidence. The parties are free to present any form of proof deemed suitable, and the judge retains unfettered discretion to assess its probative value. Judicial conviction here is guided solely by the conscience of the judge, which is not bound by statutory rules but only by the judge's own sense of certainty and fairness.

2.4. The Mixed System

Criticism of both systems has led to the emergence of a third, hybrid model. The restricted system was faulted for diminishing the role of the judge and reducing him to a passive enforcer of statutory prescriptions, while the free system raised concerns about excessive judicial discretion and the attendant risk of arbitrariness and infringement of individual rights. In response, legislators in many jurisdictions sought to combine elements of both systems, thereby creating a mixed model aimed at reconciling legislative control with judicial discretion and safeguarding the rights of the accused.

2.5.The Position of Islamic Law

Islamic jurisprudence established an evidentiary principle that "the burden of proof rests upon the claimant, and the oath is upon the one who denies." This principle, rooted in equity and fairness, reflects a structured yet balanced approach to criminal proof.

2.6. The Position of Algerian Law

The Algerian legislator has combined the free system with the restricted system, and it can be said that it has adopted the mixed system, through the provisions of Article 349 of the Code of Criminal Procedure, to which electronic evidence was added in the latest law of 2025 as a qualitative leap in the field of criminal evidence in Algeria, since this article stipulates that "crimes may be proven by any means of proof, including electronic means, except in cases where the law provides otherwise, and the judge may make his decision based on his own conviction."³.

3. Electronic Evidence as a Mechanism of Substantive Criminal Protection

In this section, we examine electronic evidence as an emerging category of criminal proof that plays a decisive role in ensuring substantive criminal protection. The rapid expansion of cybercrime and offences committed through information and communication technologies has necessitated the recognition of electronic evidence as a distinct evidentiary mechanism. Accordingly, this section is divided into two parts:

- **3.1 The Concept and Nature of Electronic Evidence**
- **3.2 Electronic Evidence as a Means of Substantive Criminal Protection**

3.1 The Concept and Nature of Electronic Evidence

Electronic evidence may be broadly defined as any information of probative value that is stored, transmitted, or generated in digital form through information and communication technologies. Unlike traditional forms of evidence, which are tangible and visible, electronic evidence is inherently intangible, volatile, and susceptible to alteration. Its authenticity and integrity therefore depend on specialized procedures for collection, preservation, and presentation.

The unique characteristics of electronic evidence—its immateriality, vulnerability to tampering, and dependence on technological devices—distinguish it from conventional evidence and justify its separate treatment within the Algerian legal framework. Comparative legislation, including French, Egyptian, and Anglo-American systems, has progressively adapted evidentiary rules to accommodate the peculiarities of digital proof. The Algerian legislator has similarly sought to recognize electronic evidence as a valid mechanism within criminal proceedings.

3.2 Electronic Evidence as a Means of Substantive Criminal Protection

The recognition of electronic evidence serves not merely procedural convenience but a substantive function: safeguarding public order and the security of society against technologically facilitated offences. By enabling prosecutors and courts to rely on digital data, surveillance outputs, and other electronically generated records, the legislator strengthens the evidentiary arsenal available to combat cybercrime, financial fraud, terrorism, and other complex offences committed through technological means.

At the same time, the integration of electronic evidence must respect substantive guarantees. These include:

- Authenticity and integrity, ensuring that digital data presented in court has not been altered.
- Reliability, requiring that the technological processes used to collect and store data are scientifically sound and legally supervised.

- Respect for rights and freedoms, particularly the rights of the defence and the protection of personal data.

Thus, electronic evidence functions as a dual mechanism: it enhances the effectiveness of criminal prosecution while preserving substantive guarantees of legality and fairness.

4. Rules of the Criminal Evidence System

Criminal proof is governed by a set of general rules that define its scope and ensure its proper application within criminal proceedings. The Algerian legislator, consistent with comparative models, has articulated several foundational principles, which may be summarized as follows:

4.1 Principle of Freedom of Evidence

Article 349 of the 2025 Code of Criminal Procedure stipulates that "offenses may be proven by any means of evidence, including electronic evidence." This principle was adopted by the legislature from the Criminal Freedom of Evidence System. The same article specifies, in the following paragraph, "Except in cases where the law provides otherwise." The legislature has exempted these offenses here because their proof requires special legal procedures, such as the crime of adultery and the crime of drunk driving, for example..

4.2 The Principle of the Judge's Intimate Conviction

This principle has received an excellent place in the eyes of the Algerian criminal legislator, and this is what we notice from the last paragraph of Article 349 of the Code of Criminal Procedure of 2025, which provides that "the judge may render his judgment based on his own conviction", because the legislator took this principle from the mixed system, and the restrictions that apply to this previous principle are the presentation of evidence in session and their discussion before the judge, and this is what paragraph 02 of the same article stipulates that "the judge may only base his decisions on the evidence that was presented to him during the pleadings and that was discussed in his presence", this evidence that was dealt with in Articles 350 of the same law, such as confession, testimonies and other evidence.

4.3 The Principle of the Legitimacy of Evidence

The admissibility of evidence is contingent upon its lawful acquisition. Evidence must not be obtained in violation of statutory provisions or in disregard of the rights of the defence. The use of coercion, force, or unlawful methods is strictly prohibited unless expressly authorized by law. This principle ensures that the search for truth does not come at the expense of fundamental procedural safeguards.

4.4 Interpretation of the rule of doubt in favor of the accused.

The Rule of Doubt (In Dubio Pro Reo) Another fundamental principle of criminal proof is that doubt must always be interpreted in favor of the accused. This rule is a direct corollary of the presumption of innocence, enshrined in Article 56 of the Algerian Constitution, which affirms that “every person is presumed innocent until proven guilty by a regular judicial authority.” The constitutional text further strengthens this safeguard by guaranteeing the right to a fair trial and the necessary means of defence.

Islamic law also recognizes this principle, as jurists hold that “al-asl bara’a” (the presumption is innocence), a principle derived from the jurisprudential maxim of *istishab* (continuity of the existing state). Comparative constitutional and international law equally affirm this principle. It appears in Article 9 of the French Declaration of the Rights of Man and of the Citizen (1789), Article 11 of the Universal Declaration of Human Rights (1948), and Article 14 of the International Covenant on Civil and Political Rights (1966). It has also been incorporated into regional instruments such as the European Convention on Human Rights (1950) and the African Charter on Human and Peoples’ Rights (1981).

5. Electronic Evidence as a Mechanism for Objective Criminal Protection

Cybercrime, by its inherent characteristics, stands apart from conventional criminality. Its dematerialized, transnational, and highly technical nature necessitates reliance on advanced evidentiary methods, foremost among them electronic recording and surveillance technologies. The distinctive features of such crimes call for a reassessment of evidentiary mechanisms in order to ensure effective criminal protection while safeguarding fundamental rights.

Accordingly, this section examines two interrelated aspects: first, the evidentiary role of optoelectronic devices in criminal proceedings and the legislative and regulatory framework governing the lawful use of audio-visual surveillance technologies in Algerian law .

5.1. The Use of Optoelectronic Devices in Criminal Evidence

This subsection explores the historical development of optoelectronic devices, their legal recognition in jurisprudence and comparative law, and their specific regulation within the Algerian legal order.

5.1.1. Evolution of the Concept of Optoelectronic Devices

Photography has long been recognized as a valuable forensic tool. Numerous jurisdictions—including the United States, the United Kingdom, Germany, and, in the Arab world, Egypt—have integrated photography into evidentiary practice, giving rise to the specialized science of forensic photography. This discipline has proven instrumental in identifying perpetrators of arson, traffic accidents, and explosives-related crimes through photographic recovery and analysis.

While early photographic techniques focused primarily on frontal identification, the French scientist Alphonse Bertillon revolutionized the field by developing profile photography and various zooming methods. His innovations paved the way for the emergence of surveillance cameras, now ubiquitous in both public and private spheres. Their utility in crime prevention and detection is well-established: New York City, for instance, was among the first metropolitan centers to install surveillance cameras as early as 1971, with the practice subsequently adopted worldwide.⁴

5.1.2. The Legal Use of Optoelectronic Devices in Jurisprudence and Comparative Law

The increasing deployment of surveillance technologies by state authorities, and their gradual extension to private use, has inevitably raised concerns regarding the protection of privacy. Jurisprudence has been divided on this issue. Some scholars have argued that the prohibition on unauthorized searches is inapplicable to visual surveillance, whereas others have insisted on robust safeguards for individual freedoms, emphasizing that investigative powers should not be extended from the material to the immaterial sphere without clear legal authority.

A central issue in this debate is whether the person under surveillance must be notified. On the one hand, notification enhances transparency and the protection of rights; on the other hand, it risks compromising investigations by alerting suspects, thereby endangering the evidentiary process. To reconcile these competing imperatives, most comparative legislations have introduced strict controls on visual surveillance. Failure to comply renders the evidence inadmissible and constitutes a violation of constitutionally protected rights and freedoms. Notable examples include U.S. legislation of 1968, which excluded evidence obtained in violation of privacy, and the French law of 1995, which similarly circumscribed surveillance powers.⁵

5.1.3. The Legal Use of Optoelectronic Devices in the Algerian Legal System

Algerian law draws a distinction between surveillance conducted by state authorities under the National Video Surveillance System and surveillance conducted by private individuals⁶.

A- Surveillance under the National Video Surveillance System

Presidential Decree No. 15-228 of 22 August 2015 governs the organization and operation of the National Video Surveillance System. Placed under the supervision of the Prime Minister, the system operates through provincial centers located within each governorate and accessible to the Wali.⁷

Article 2 of the Decree enumerates seven principal purposes: combating terrorism; preventing criminal acts; protecting persons and property; maintaining public order; monitoring traffic and detecting violations; securing sensitive facilities; and managing crises or natural disasters.

Article 4 designates the geographical scope of surveillance, including major urban and peri-urban centers, major roadways (particularly those with high traffic), and public spaces. Notably, the Decree does not require prior authorization for the installation of cameras in public areas or spaces open to the public. However, where cameras are used to monitor public roads adjacent to private business establishments, prior authorization from the Wali is required.

B- Use of Surveillance Cameras by Individuals for Sensitive Installations

Private individuals are also authorized to employ surveillance technologies in connection with sensitive installations. This practice is regulated by Executive Decree No. 09-410, as amended and supplemented, which establishes security regulations for sensitive equipment.⁸

Under Section C, surveillance cameras are classified as “special sensitive equipment” and divided into two categories: fixed video surveillance devices (excluding those with night-vision capabilities, which are subject to specific provisions)⁹; and mobile surveillance devices. Licenses are issued by the competent Wali at the regional level, following submission of an application and completion of a security review.

6. The Legal Use of Audio Recording and Listening Devices under Algerian Law

The Algerian legislature has expressly regulated the use of audio recording and listening devices within the framework of criminal proceedings. These provisions were introduced through the 2006 amendment to the Code of Criminal Procedure, particularly Articles 65 bis 5 and following, which establish both substantive and procedural conditions for admissibility.

The Criminal Procedure Code of 2025 provides for various procedures relating to voice recording and taking of photographs, as contained in Article 114 and subsequent sections of Chapter Four, which relate to the interception of correspondence, voice recording and taking of photographs, in accordance with specific formal and substantive conditions.

6.1. Objective conditions

The legislator has imposed a set of objective conditions, which are as follows ;

- If the requirements of the flagrante delicto investigation ,
- Preliminary investigations into offenses involving intentional homicide, narcotics and psychotropic substances, transnational organized crime, offenses related to information and communication technologies, money laundering, terrorism, and offenses related to foreign exchange and capital movements to and from abroad, corruption, smuggling, human trafficking, organ trafficking, migrant smuggling, and kidnapping of persons.

6.2. Procedural conditions

Article 114 of Law 25-14 on the Code of Criminal Procedure defines these procedures as follows:

- Intercepting correspondence via wired or wireless communication means.
- Implementing technical arrangements, without the consent of the parties concerned, to capture, record, transmit, or transmit speech spoken privately or confidentially by one or more persons in private or public places, or to take photographs of one or more persons present in a private place.
- This may only be done with a written judicial authorization under the supervision of the competent public prosecutor, for a maximum period of four months, renewable according to the requirements of the investigation or inquiry, as stipulated in Article 116/2 of the Code of Criminal Procedure.
- This authorization, for the purpose of establishing the necessary technical arrangements, allows entry into any residential or other premises, even outside the hours stipulated in Article 78 of this law, without the knowledge or consent of the property owners.
- Authorized operations must be carried out under the direct supervision of the competent public prosecutor.
- In the event of a judicial investigation, this authorization is granted by the investigating judge. Authorized operations must be carried out under his direct supervision.

7. Procedural Mechanisms for the Use of Electronic Evidence in Algeria

The Algerian legislator has complemented substantive provisions on electronic evidence with procedural mechanisms designed to ensure its effective and lawful use in criminal proceedings. Chief among these are: the establishment of a national criminal unit specializing in offenses related to information and communication technologies, and the regulation of judicial jurisdiction and modalities for the exercise of authority within this specialized unit.

7.1. Creation of a National Criminal Unit to Combat ICT-Related Offenses

The establishment of a specialized criminal division dedicated to ICT-related offenses was not an isolated initiative but the culmination of a progressive legislative trajectory. The groundwork was laid by Law No. 09-04 of 5 August 2009, which introduced special rules for the prevention and suppression of crimes committed through information and communication technologies, while the formal creation of the judicial division was subsequently enshrined in the 2021 amendment to the Code of Criminal Procedure.

7.2. Preparatory Framework: Law No. 09-04

Law No. 09-04 sought to define the legal contours of ICT-related offenses and to introduce rules for their prevention and prosecution. While the Criminal Code already penalized infringements of automated data processing systems, Law No. 09-04 broadened the scope to encompass other forms of criminal conduct committed or facilitated through electronic communication systems.¹⁰

The law provided legal definitions essential for the classification of ICT-related offenses, including:

- **Information System:** Any discrete system, or interconnected group of systems, in which one or more components automatically process data in accordance with a specified program.
- **Information Data:** Any representation of facts, information, or concepts in a form suitable for processing within an information system, including the software enabling the system to perform its functions.
- **Service Providers:** Defined consistently with Law No. 18-07, these include:
 - o any public or private entity offering its users the capacity to communicate via an information or communication system;
 - o any entity that processes or stores information data on behalf of such a service or its users.
- **Traffic Data:** Data generated by an information system in the context of a communication cycle, identifying the source, destination, routing, date, time, duration, volume, and type of service employed.
- **Electronic Communications:** The transmission or reception of signs, signals, texts, images, sounds, or other forms of information by electronic means.¹¹

Through these definitions, Law No. 09-04 provided the conceptual architecture necessary for the recognition of electronic evidence and set the stage for the later procedural reforms of 2021, which institutionalized a specialized judicial division with jurisdiction over ICT-related criminality.

7.3. The Institutionalization of the National Criminal Division under the 2021 Amendment

It was initially included in Ordinance 21-11 of August 25, 2021, amending the Code of Criminal Procedure for the year 2021, by which a sixth chapter was included under the name of “National Criminal Unit for the Fight against Offenses Related to Information and Communication Technologies”.¹²

The 2025 Code of Criminal Procedure preserved this body, and given the seriousness of these crimes, as they constitute a threat to the safety of people and property, the legislator therefore assigned it special deterrent measures, in accordance with Law 25-14 of 08/03/2025 on the Code of Criminal Procedure, by which a third chapter of the fourth title relating to criminal judicial centers was included under the name of "National Criminal Center for the Fight against Offenses Related to Information and Communication Technologies".¹³

Provides that there is, within the jurisdiction of the High Council of the Judiciary of Algiers, a national criminal unit specializing in the prosecution and investigation of offenses related to information and communication technologies and related offenses. It is also competent to rule on the offenses provided for in this chapter if they constitute crimes.¹⁴

By which the legislator considered that the concept of offences related to information and communication technologies is the offence committed or facilitated by the use of an

information system, an electronic communications system or any other means or mechanism related to information and communication technologies.¹⁵

The Prosecutor at the National Criminal Division for the Fight against Offenses Related to Information and Communication Technologies, as well as the investigating judge and the head of the same division, exercise their powers throughout the national territory.¹⁶

The prosecutor of the National Criminal Division for Combating Offenses Related to Information and Communication Technologies, the investigating judge, and the head of this division are exclusively responsible for prosecuting, investigating, and judging the offenses exclusively related to information and communication technologies listed below, as well as related offenses:

- Offenses threatening state security or national defense;
- Offenses involving the publication and dissemination of false news likely to undermine security, public tranquility, or social stability;
- Offenses involving the publication and dissemination of biased news that undermine public order and security, whether organized or cross-border;
- Offenses involving interference with the automated data processing systems of public administrations and institutions;
- Offenses involving trafficking in human beings, human organs, or migrant smuggling;
- Offenses involving discrimination and hate speech.¹⁷

The prosecutor of the National Criminal Division for Combating Offenses Related to Information and Communication Technologies, as well as the investigating judge and the head of this division, are exclusively responsible for prosecuting, investigating, and judging the most complex offenses related to information and communication technologies and related offenses.¹⁸

For the purposes of this law, a most complex offense related to information and communication technologies means an offense which, due to the multiplicity of perpetrators, accomplices, or victims, the geographical scope of its commission, the seriousness of its effects or resulting damage, its organized or transnational nature, or its threat to public order and security, requires the use of special investigative methods, specialized technical expertise, or international judicial cooperation.

7.4 Determination of the Procedures for Exercising Judicial Jurisdiction Before the Competent Criminal Unit

The prosecutor of the National Criminal Unit for Combating Offenses Related to Information and Communication Technologies, as well as the investigating judge and the head of the same unit, exercise jurisdiction concurrently with the jurisdiction resulting from

the application of Articles 58, 70, and 329 of the Code of Criminal Procedure with regard to offenses related to information and communication technologies and related offenses, as provided for in Article 340 of the Code of Criminal Procedure.

In this case, the procedures provided for in Articles 317 to 329 of the same law apply before the National Criminal Unit for Combating Offenses Related to Information and Communication Technologies.¹⁹

If the jurisdiction of the National Criminal Unit for Combating Offenses Related to Information and Communication Technologies coincides with that of the Economic and Financial Unit, jurisdiction is necessarily transferred to the latter.²⁰

The same applies if the jurisdiction of the National Criminal Unit for the Fight against Offenses Related to Information and Communication Technologies coincides with the jurisdiction of the National Criminal Unit for the Fight against Terrorism and Transnational Organized Crime, in which case jurisdiction will necessarily be transferred to the latter, as provided for in Article 342 of the Code of Criminal Procedure.²¹

Conclusion

It is clear that electronic evidence has become a decisive and indispensable element in contemporary criminal proceedings, particularly in light of the exponential rise of cybercrime worldwide. The probative value of such evidence has not only reshaped evidentiary practices but has also contributed to the evolution of the very concept of cybercrime, this is what the legislator confirmed through the explicit recognition of electronic evidence in the Criminal Procedures Law of 2025.

At the procedural level, Algeria has made significant strides by granting extensive powers to the specialized judicial division for combating ICT-related offenses, as established under Law No. 09-04 and reinforced by subsequent legislative reforms. These measures reflect the legislature's recognition of the strategic importance of electronic evidence in ensuring effective criminal protection.

Nevertheless, to consolidate the role of electronic evidence in Algeria's legal system, further efforts are required. Criminal data must be safeguarded through robust technical protection mechanisms integrated within automated data processing systems. Equal emphasis should be placed on the human factor, by training and equipping specialized personnel capable of detecting, investigating, and prosecuting cybercrimes. Comparative monitoring of foreign criminal justice systems, alongside enhanced regional and international cooperation, is essential to exchange expertise and adopt best practices.

Moreover, the expansion of video surveillance beyond major urban centers to all districts would significantly strengthen preventive measures, provided that such systems remain subject to clear legal safeguards. Facilitating the licensing process for private

individuals to use surveillance technologies can also contribute to wider community protection.

A further challenge lies in achieving legislative harmony between privacy rights and collective security requirements. Reconciling these interests demands coherent legal drafting that avoids fragmentation. In this respect, a unified framework should be sought by bridging the provisions of Law No. 18-07 on the protection of personal data with those of Law No. 09-04 on ICT-related offenses.

Ultimately, legal certainty remains the cornerstone of an effective justice system. It can only be guaranteed through the establishment of a robust cybersecurity infrastructure, supported by a legislative framework that elevates electronic evidence to its rightful place within Algeria's criminal justice system. Such reforms will not only enhance the fight against cybercrime but also consolidate Algeria's broader policy objectives, including the protection of investments, financial transactions, and the security of individuals and property.

Citations:

- 1-Kara Amel, cybercriminalité, Master in droit pénal and sciences criminelles, faculté de droit, université d'Alger, 2005, p. 1.
- 2- Rabine Donia, Evidence by Indirect Evidence in Criminal Matters, Master's Degree in Criminal Law and Criminal Sciences, Faculty of Law, Algeria, 2015, p. 7.
- 3- Law n° 25-14 of 03/08/2025, relating to the Code of Criminal Procedure, Official Journal of the Algerian Republic, No. 54 of 13/08/2025, p. 07.
- 4-Nour El Houda Mahmoudi, The legitimacy of modern scientific methods in criminal evidence, Doctorate in criminology and penology, University of Batna, Algeria, 2018, p. 248.
- 5-Same reference, p. 257.
- 6-Presidential Decree n°15-228 of 22/08/2015 establishing the general rules relating to the organization and operation of the national video surveillance system, Official Journal of the Algerian Republic, No. 45 of 23/08/2015, p. 03.
- 7-Article 07 of Presidential Decree 15-228, same reference, p. 04.
- 8-Executive Decree n°09-410 of 10/12/2009 Setting the safety rules applicable to activities involving sensitive equipment. Amended and supplemented by Executive Decree No. 16-61 of 11/02/2016, Official Journal of the Algerian Republic, No. 09 of 17/02/2016.
- 9-Night vision surveillance equipment is subject to the provisions of Executive Decree No. 98-96 of 18/03/1998, amended and supplemented, which determines the terms of application of Order n° 97-06 of 21/01/1997, relating to military equipment, weapons and ammunition
- 10- Official Journal of the Algerian Republic, No.47 of 08/16/2009, p. 05
- 11- Article 02 of Law 09-04.
- 12- Official Journal of the Algerian Republic, No.65 of 26/08/2021, p. 07.
- 13- Official Journal of the Algerian Republic, n° 54 of 13/08/2025, previous reference, p. 49.
- 14- Article 335/1 of Law 25-14, same reference, p. 50.
- 15- Article 335/2 of Law 25-14, same reference, p. 51.
- 16-Article 336 of Law 25-14, Official Journal of the Algerian Republic, No.54.Official Journal of the Algerian Republic,No.54 dated 08/13/2025, previous reference, p. 49, p. 50.
- 17- Article 337 of Law 25-14, same reference same page.
- 18- Article 338 of Law 25-14, same reference same page.
- 19-Article 340/2 of the Code of Criminal Procedure, previous reference, p. 50.
- 20- Article 341 of Law 25-14 containing the Code of Criminal Procedure, same reference, same page.
- 21- Same reference, same page, this pole which was addressed in the fourth chapter.