

Proof With Digital Evidence Between Privacy Guarantees and Authenticity Requirements: A Fundamental Study in Light of the Algerian Code of Criminal Procedure

ANSEUR Lahouaria *

Associate Professor Classe A University of Oran 2 -Mohamed Ben Ahmed-, Faculty of Law and Political Science, Investment and sustainable development laboratory

Email: anseurlahouaria@gmail.com

Received: 10/01/2026 Accepted: 28/06/2026 Published: 01/07/2026

Abstract

Digital transformation has profoundly changed the nature of crime and the methods used to commit it, which has significantly affected the rules of criminal evidence. Digital evidence, including electronic data, communications, recordings, and connection data, has become an important means of detecting crimes and establishing criminal responsibility. This study aims to examine the concept of digital criminal evidence and highlight the specific characteristics of electronic evidence, while analyzing the extent to which Algerian Code of Criminal Procedure No. 25-14 of August 3, 2025 responds to the requirements of the digital environment. The study also addresses the legality of collecting, preserving, and examining digital evidence, its evidentiary value before criminal courts, the limits of judicial discretion, and the procedural safeguards established to protect individual rights and freedoms. The study emphasizes the need to balance effective crime prevention and the use of technological developments with respect for procedural legality, privacy, and the rights of the defense. It concludes that developing digital evidence mechanisms and strengthening legal and technical safeguards are essential to ensure the reliability and admissibility of digital evidence before courts.

Keywords : Criminal Evidence ; Digital Evidence ; Digital Transformation ; Code of Criminal Procedure; Cybercrime

Introduction

In recent decades, the world has witnessed a profound transformation due to the widespread spread of information and communication technologies, and the transfer of a large part of human activity from the traditional physical sphere to the digital sphere. Social, economic, administrative, and judicial relations are no longer immune to this transformation. Rather, daily transactions have become increasingly dependent on electronic media, whether related to communications, commercial exchange, banking services, information storage, or social networking.

This transformation was directly reflected in the criminal phenomenon. Crime is no longer committed by traditional means alone, but the digital space has become a field for committing new crimes, and technology has become an aid in committing traditional crimes. It has become possible for a person, institution, or information system to be attacked from a

remote location, and for the crime to leave digital traces that are imperceptible in the traditional sense, but can be extracted, analyzed, and used before the judiciary.

In the face of this development, criminal proof faces a real challenge. Because the evidence that the investigating authorities are looking for may not be a physical object in the usual sense, but rather it may be a digital file, an electronic message, a communication record, data stored in a smartphone, information saved in an electronic server, or content published via a social network. Hence, what is known as digital or electronic evidence emerged as one of the most important aspects of the development of criminal evidence in the digital environment.

The problem is not limited to recognizing digital evidence in theory, but rather extends to how to obtain it, preserve it, verify its integrity, attribute it to its owner, present it before the judiciary, and discuss it before the opponents. Digital evidence is characterized by the ease of copying, modifying, deleting and transferring, which makes maintaining its integrity and authenticity a central issue in determining its evidentiary value.

Algerian legislation, in turn, witnessed gradual development in this field. In addition to the general provisions related to proof, the legislator adopted a set of texts aimed at confronting crimes related to information and communication technologies, most notably Law No. 09-04 of August 5, 2009, which includes special rules for preventing and combating crimes related to information and communication technologies.

The legislator also recognized the importance of the electronic environment through Law No. 15-04 of February 1, 2015, which defines the general rules related to electronic signature and authentication, as it approved a legal framework for this field aimed at ensuring trust and security in electronic transactions.

Then came Law No. 25-14 of August 3, 2025, which includes the Code of Criminal Procedure, to establish a new procedural framework. It is a law based in its first article on the principles of legality, fair trial, and respect for human dignity and rights, making dealing with digital means necessarily subject to these basic principles.

Hence, the importance of studying the relationship between digital transformation and criminal proof emerges, not only as a technical issue, but as a legal and constitutional issue directly related to the protection of private life, the sanctity of correspondence, the rights of defense, and the presumption of innocence.

The problem of the study

Based on the above, the main problem of the study can be formulated as follows:

To what extent was the Algerian legislator able, in light of Law No. 25-14, which includes the Code of Criminal Procedure, to establish digital criminal evidence, regulate the procedures for obtaining electronic evidence, and ensure its validity before the judiciary, in a way that achieves a balance between the effectiveness of combating digital crime and protecting basic rights and freedoms ?

A number of questions arise from this problem, the most important of which is:

1. What is meant by digital evidence and what are its most important characteristics?
2. What is the legal basis for digital proof in Algerian legislation?
3. What are the most important legal procedures for collecting digital evidence?
4. What are the controls governing the legality of electronic evidence?

5. How authoritative is digital evidence before a criminal judge?
6. How can a balance be achieved between the effectiveness of digital investigation and the protection of private life and defense rights?

Accordingly, the topic will be addressed through two sections:

The first topic: the legal foundation of criminal evidence in the digital environment

Crime in the modern era has witnessed a remarkable transformation due to the rapid development in information and communications technology, as digital means and information systems have become an essential part of various forms of criminal activity, whether in terms of committing the crime or in terms of storing information and traces that can reveal its circumstances. This has resulted in the emergence of a new type of evidence that differs in nature and characteristics from traditional evidence, which is called digital or electronic evidence.

The emergence of this type of evidence has imposed new challenges on the rules of criminal evidence, especially with regard to defining the concept of digital evidence, clarifying its legal nature, and the extent of its authority before the judiciary, as well as the controls and procedures that must be respected when collecting, preserving, examining and submitting it. Protecting the integrity of evidence from alteration or tampering, and ensuring the legality of obtaining it, have also become fundamental issues that affect its evidentiary value.

Accordingly, this study aims to clarify the legal basis for criminal proof in the digital environment, by examining the concept of digital evidence and its privacy, and then studying the legislative basis that regulates reliance on it in the criminal field.

The first requirement: the concept of digital evidence and its privacy

The digital environment has produced new forms of traces that can infer the occurrence of a crime, identify its perpetrator, or prove his connection to the criminal act. Data stored in computers, phones, and electronic media, along with messages, conversations, digital recordings, and system records, have become important sources of information of criminal value. However, these effects differ from traditional evidence in terms of their nature, the means of production, and the method of accessing them.

Defining the concept of digital evidence is of particular importance, because defining the term constitutes the basis for determining its scope and distinguishing it from other evidence, and its technical nature gives it a set of characteristics that affect how it is collected, preserved, analyzed, and presented before the judiciary. Digital evidence is characterized, among other things, by its ability to be copied, transferred, modified and deleted, and in many cases by its need for specialized technical means and tools to extract and read it.

Accordingly, this requirement will be addressed by clarifying the concept of digital evidence first, and then examining its specificity and characteristics second, allowing it to determine its nature and role within the contemporary criminal evidence system.

The first section: The concept of digital evidence

Digital evidence means all information or data with probative value that is created, stored, circulated, or extracted by an information system or electronic means, and can be used

to detect the crime, identify its perpetrator, or prove the relationship between the crime and its perpetrator.¹

This includes a wide range of images, including digital files, emails, conversations, photos, audio and video recordings, logs into systems, geo-location data, communications data, the contents of smartphones and computers, as well as information circulated through social media platforms.

Digital evidence does not necessarily mean that the crime associated with it is a cybercrime; Digital evidence may be used to prove a traditional crime, such as geographical location data revealing the presence of a person at the place where the crime was committed, or an electronic message revealing the existence of a prior agreement between a group of people.

Hence, the scope of digital evidence is broader than that of cybercrime, because it can be evidence in both cybercrimes and traditional crimes.

Algerian legal studies have confirmed that electronic evidence has become an important means of proving crimes, and that its validity is linked to the extent of respect for the procedures for obtaining it and discussing it before the judiciary and the extent to which its integrity and certainty can be verified.²

Section Two: Characteristics of digital evidence

Digital evidence is characterized by a set of characteristics that give it a special nature in the field of criminal evidence.

First: non-material nature

Digital evidence is often not tangible in itself, but rather appears through a technical means that allows it to be read or viewed. The file on the computer does not in itself represent the image that a person sees, but rather the digital data is converted into content that can be perceived by specific programs and devices.

Second: ease of copying

Digital evidence can be copied multiple times without the copying itself changing the substance of the data, which distinguishes it from some traditional evidence that is tied to the physical original.

Third: Ability to modify and delete

One of the most important problems of digital evidence is the possibility of quickly modifying or deleting data, which imposes the necessity of taking technical and legal measures to preserve the integrity of the evidence from the moment it is seized until it is presented before the court.³

Fourth: The possibility of its transmission across borders

The data needed by the investigation may be held in another country or with a company providing digital services outside the national territory, which raises issues of jurisdiction, international cooperation and information exchange.

Fifth: Its connection to technical expertise

Interpreting some digital evidence requires specialized technical knowledge, as the judge may not be able to determine on his own how to extract the data or ensure that it has not been altered, making technical expertise extremely important.

The second requirement: The legal basis for digital proof in Algerian legislation

The increasing spread of the use of digital means in various areas of life has imposed new challenges on the Algerian legislator, especially in the criminal field, as traditional means of proof alone are no longer sufficient to confront crimes committed using information and communication technologies. It has become necessary to create a legal framework that allows dealing with evidence derived from digital devices, systems and networks, while ensuring its legitimacy and the integrity of the procedures for obtaining, preserving and presenting it before judicial authorities.

In this context, Algerian legislation has gradually tended to enshrine a set of legal rules that allow electronic means and digital data to be relied upon in the field of proof, whether through general rules related to criminal proof, or through special texts on combating crimes related to information and communication technologies, as well as provisions related to signature, electronic commerce, and data protection related to the digital environment. The Code of Criminal Procedure, along with special legislation, has become an important framework for regulating the means of research and investigation that can produce digital evidence.

The importance of studying the legal basis for digital evidence in Algerian legislation lies in determining the extent to which the legislator recognizes this type of evidence, and explaining the rules that govern the legality of its collection, seizure, examination and preservation, and the extent to which it enjoys probative power before the criminal judiciary. This issue also raises the problem of reconciling the effectiveness of combating digital crime, on the one hand, and respecting individual rights and freedoms, most notably the right to privacy, confidentiality of correspondence, and protection of personal data, on the other hand.

Accordingly, research into this requirement requires examining the various Algerian legal texts regulating digital evidence, and demonstrating the extent to which the Algerian legislative system accommodates developments related to digital evidence, while highlighting the most important legal guarantees and restrictions governing its use in the criminal field.

Section One: General rules of criminal proof

Criminal proof is based on a set of basic principles that aim to reach the judicial truth while preserving the rights of the accused and the guarantees of a fair trial.

Since its first article, the new Criminal Procedure Law No. 25-14 has affirmed the procedural system's connection to the principles of legality, fair trial, and respect for human dignity and rights. It also establishes the presumption of innocence and the inadmissibility of punishing a person except on the basis of proving his responsibility according to the law.

These principles gain special importance in the digital environment, because the use of technology to search for evidence may lead to compromising private life or the confidentiality of correspondence or personal data if it is not restricted by precise legal controls.

Therefore, recognizing digital evidence does not mean granting investigative authorities absolute freedom to access all electronic data, but rather it must be obtained in accordance with legal procedures that respect the principle of legality.⁴

Section Two: Combating digital crimes

Law No. 09-04 of August 5, 2009 constituted an important point in the development of Algerian criminal policy towards crimes related to information and communication

technologies. The legislator allocated this law to establish special rules to prevent and combat crimes related to information and communication technologies.

The importance of this law lies in the fact that it responded to the special nature of information crimes, which are difficult to deal with by traditional means alone. Digital crime may not leave a clear physical trace, but rather leaves electronic traces that require specialized technical means to discover, preserve and analyze them.

Hence, legislative policy was linked to monitoring electronic communications and obtaining the data necessary for investigation, while subjecting these procedures to legal conditions and controls.

The second section: The validity of digital evidence and guarantees of its use before the criminal judiciary

Digital evidence has become increasingly prominent in the criminal evidence system, as a result of the rapid development in the use of electronic means and the increase in crimes related to the digital space. Electronic data is no longer just technical information of limited value, but in many cases it has become an essential source for detecting criminal incidents and proving people's connection to them, through the correspondence, files, recordings, electronic records and other digital traces it contains.

However, the reliance on digital evidence before the criminal judiciary does not depend on its mere existence or the possibility of obtaining it, but rather is linked to the extent of the availability of legal and technical conditions that guarantee its safety, credibility, and the legality of obtaining it. Its nature, which can be copied, modified and deleted, imposes the need to verify that it has not been subject to distortion or tampering, and that its chain of possession is intact from the moment it is seized until it is presented before a judge.

On the other hand, the use of digital means for proof must not lead to prejudice to the basic rights and freedoms guaranteed by the law, especially the right to privacy, confidentiality of correspondence and communications, and protection of personal data. Hence, the importance of achieving a balance between the requirements of combating crime and achieving criminal justice on the one hand, and respecting the legal guarantees established for the accused and the rest of the parties to the case on the other hand.

Accordingly, this research deals with the validity of digital evidence before the criminal judiciary, and the legal and procedural guarantees associated with its use, by stating the extent of the criminal judge's conviction in it, the conditions for its acceptance, and evaluating its probative strength, then studying the most important guarantees that govern obtaining it and presenting it before the judiciary.

The first requirement: the validity of digital evidence before the criminal judge

Recognizing digital evidence as a means of criminal proof raises a fundamental issue, which is determining the extent of its authority before the criminal judge, and the extent of his ability to form his judicial conviction regarding the occurrence of the crime and its attribution to the accused. Digital evidence, despite its technical nature, does not differ in its basic function from other evidence as long as it meets the conditions of legality, safety and credibility, and the judge can verify its source, authenticity and connection to the facts under investigation.

The importance of this issue increases in view of the principle of freedom of criminal proof and judicial conviction, as the judge has, within the limits set by the law, the authority to evaluate the evidence presented to him and take what reassures his conscience, provided that his conclusion is based on legal and logical reasons. Therefore, the probative value of digital evidence is not only related to its electronic nature, but also to the soundness of the procedures for obtaining, preserving and examining it, and to its ability to withstand judicial discussion.

Digital evidence also requires the criminal judge to deal with technical issues that may require the use of technical expertise, especially when it comes to examining electronic devices, retrieving deleted data, or verifying the source of communications and digital files. Hence the necessity of determining the criteria for evaluating this evidence, and clarifying the extent of the judge's independence in assessing its probative strength, and the extent to which defects that may mar the process of collecting, preserving, or analyzing it affect its authenticity.

Accordingly, through this requirement, the extent of the validity of digital evidence before the criminal judge, the conditions for its acceptance, and the criteria for estimating its evidentiary strength will be examined, with an explanation of its role in forming judicial conviction in light of the developments witnessed by modern means of criminal proof.

The first section: the principle of freedom of criminal proof

Criminal proof in Algerian legislation is linked to the principle of freedom of proof and judicial conviction, where evidence is not limited to rigidly defined means, but rather the judge has the authority to evaluate the evidence presented to him in accordance with the law.

This rule constitutes an important basis for accepting digital evidence, because the absence of a special designation for each type of digital evidence does not necessarily mean that it cannot be relied upon.

Algerian studies have concluded that the criminal judge has discretionary power in dealing with electronic evidence, but this power is not absolute, but must be exercised in accordance with the law, judicial logic, and fair trial guarantees.

Therefore, digital evidence can have probative value whenever it is legitimate, valid and arguable, but this does not mean that it has absolute probative force.⁵

Section Two: The principle of judicial conviction

Judicial conviction means the state of mind that the judge reaches after examining the elements of the case and the evidence presented to him.

In the digital environment, the role of judicial conviction becomes increasingly important due to the technical nature of the evidence, as the judge may be faced with a large amount of data whose legal significance can only be understood through technical analysis.

The judge remains the final decision maker in assessing the value of the evidence, but he must distinguish between:

- existence of evidence;
- The validity of the evidence;
- integrity of evidence;
- Attribution of evidence to the accused;

- The relationship between evidence and crime;
- The sufficiency of the evidence to establish judicial conviction.

These elements confirm that the presence of an electronic message, for example, alone is not sufficient to prove the commission of a crime, unless the identity of its sender, the integrity of its content, and its connection to the facts under investigation are confirmed.⁶

The second requirement: Conditions for accepting digital evidence

It is not sufficient for digital evidence to be considered a valid means of criminal proof simply by obtaining it from an electronic device or information system, but rather it must meet a set of legal and technical conditions that guarantee its legitimacy, validity, and safety of its content. The privacy of the digital environment, and its ease of copying, modifying, deleting and transferring data, makes it necessary to subject digital evidence to precise controls that ensure that its content is not compromised or its characteristics are changed during the stages of collection, examination and analysis.

Respecting the legality of obtaining evidence is one of the most important conditions for its admission before the judiciary, as it must be collected in accordance with the procedures specified by law, and without unlawfully violating basic rights and freedoms, especially the right to privacy, confidentiality of correspondence and communications, and protection of personal data. The nature of digital evidence also requires the need to ensure its authenticity and integrity, by verifying its source and verifying that it has not been subject to modification or distortion from the moment it is seized until it is presented before the court.

The acceptance of digital evidence is also linked to the soundness of the technical procedures used in extracting, preserving and analyzing it, and to the possibility of documenting the various stages it has gone through, which allows proving the continuity of its possession and preserving its original characteristics. In this context, the importance of technical expertise and approved technical tools is highlighted, given that some forms of digital evidence cannot be understood or verified except with the help of specialized scientific and technical means.

Hence, the acceptance of digital evidence before the criminal judiciary is based on an integrated set of controls, intertwined with legal legitimacy, authenticity, technical integrity, reliability, soundness of seizure and preservation procedures, and the susceptibility of the evidence to judicial discussion. Accordingly, through this requirement, we will study the most important conditions that must be met in the digital evidence in order for it to be valid for reliance on it in criminal proof, while explaining the consequences of violating these conditions.

The first section: The legality of obtaining evidence

Legality is the first condition for accepting digital evidence, and it means that the evidence was obtained by a competent authority and in accordance with procedures specified by law, without an unlawful attack on rights and freedoms.

Technology cannot eliminate the guarantees established by law for individuals, but must be used within the framework of those guarantees.

It follows that evidence obtained illegally may become the subject of discussion before the judiciary, depending on the nature of the procedure and the texts regulating it.⁷

Section Two: Integrity of digital evidence

The integrity of digital evidence is one of the most important conditions for its validity. Given the ease of modifying electronic files, it must be possible to prove that the data submitted to the judiciary has not been distorted or tampered with.

This is achieved through the use of digital forensic techniques and tools that allow preserving the original data, and creating forensic copies to work on without changing the original.

From a legal perspective, the integrity of the evidence is not only related to the technical aspect, but is also related to proving the chain of custody, that is, identifying the people and entities that dealt with the evidence from the time it was seized until it was presented before the court.

The third section: The legal and practical challenges of digital forensic evidence and the prospects for its development

The accelerated digital transformation has created a new reality in the field of criminal evidence, making digital evidence an increasingly important element in detecting and proving crimes. However, relying on it has not been without multiple difficulties and challenges of a legal, technical and practical nature. The privacy of the digital environment, the rapid development of means of committing crimes, and the increasing volume of data circulating across systems and networks are all factors that require criminal justice agencies to develop research and investigation methods and means of dealing with evidence derived from the digital world.

The challenges facing digital criminal evidence are numerous. From a legal perspective, problems arise related to the adequacy of legislative texts to keep pace with technical developments, the limits of the legality of obtaining digital data, and protecting privacy and confidentiality of communications, in addition to the difficulties associated with cross-border crimes and determining jurisdiction and the applicable law. From a practical and technical standpoint, the difficulties are represented by the speed with which data changes or the possibility of deleting and modifying it, the difficulty of determining its source, the multiplicity of devices and systems that may contain traces of the crime, in addition to the need for human expertise and specialized technical tools to control and analyze evidence and maintain its integrity.

The continuous development in artificial intelligence, cloud computing, encryption, and Internet of Things technologies opens new areas for criminals on the one hand, and poses additional challenges for law enforcement and judiciary bodies on the other hand. Which makes developing the legal and technical framework for digital proof a continuous necessity, and not just a circumstantial response to technological development.

Accordingly, this research addresses the most important legal and practical challenges facing digital evidence, and then examines the prospects for developing the digital criminal evidence system in a way that achieves a balance between the effectiveness of combating digital crime, ensuring respect for basic rights and freedoms, and enhancing the ability of criminal justice to deal with successive technological developments.

The first requirement: Challenges facing digital evidence

Digital evidence, despite its increasing importance in the field of forensic evidence, faces a set of challenges imposed by its technical nature and the electronic environment in which it is created. Unlike traditional evidence, which often has a physical presence that can be viewed and controlled directly, digital evidence represents electronic data and information that may be stored on different devices or distributed across multiple networks and information systems, which makes accessing it, controlling it, and maintaining its integrity a process that requires technical means and precise legal procedures.

These challenges range from legal, procedural, technical and practical, as investigators may face difficulty in determining the entity or place where the data is located, especially when it is stored on servers located outside the country's territory or within cloud computing services. Cross-border digital crimes also pose problems related to jurisdiction, international cooperation, and obtaining data held by digital service providers in other countries.

On the other hand, the fragile nature of digital evidence makes it vulnerable to change, deletion, or destruction, whether intentionally by the perpetrator of the crime or unintentionally during the seizure and examination process. Therefore, any defect in the procedures for collecting, copying, storing or transporting evidence may affect its integrity and credibility, and may raise doubts about its value before the judiciary. The use of advanced encryption and protection technologies may make accessing the requested data more difficult.

The challenges are not limited to the technical aspect, but extend to the legal aspect, especially with regard to reconciling the need to enable competent authorities to access digital data in order to combat crime, and protecting the right to privacy, confidentiality of correspondence and communications, and protecting personal data. Therefore, the legality of obtaining digital evidence represents an essential element in determining the extent to which it can be relied upon judicially.

Another problem also arises, which is the lack of specialized competencies and expertise capable of dealing with digital evidence, as examining devices and systems, retrieving deleted data, and analyzing the effects of electronic activity requires specialized technical knowledge, in addition to familiarity with the legal and procedural rules that govern the evidentiary process. Therefore, the effectiveness of the digital proof system is highly related to the availability of qualified experts, digital forensic laboratories, and modern technical equipment.

Accordingly, the challenges facing digital evidence can be studied through a set of basic elements, namely: legal and procedural challenges, technical and technical challenges, challenges related to the integrity and authenticity of the evidence, challenges related to cross-border crimes, in addition to the challenges of protecting rights and freedoms and providing specialized competencies and expertise. Analysis of these challenges reveals the need for continuous development of legislation and judicial and technical practice to ensure the benefit of digital evidence without prejudice to fair trial guarantees.

The first section: The difficulty of determining the source of the evidence

It can sometimes be difficult to identify who created or sent data, especially when you use fake accounts, VPNs, or shared devices.

Therefore, the Internet address or account name does not always constitute conclusive evidence of the identity of the actor, but rather should be linked to a set of digital and physical clues.

The second section: The speed with which evidence disappears

Digital data can be deleted or modified, and the perpetrator may destroy evidence immediately upon learning of the investigation.

This requires rapid intervention, and the investigative agencies' possession of technical mechanisms that allow the preservation of evidence before it disappears.

The second requirement: Evaluation of the Algerian regulation of digital proof

It can be said that Algerian legislation has made important strides in dealing with digital transformation in the criminal field.

It moved from almost complete reliance on traditional means to recognizing technical means of research and investigation, especially through Law No. 09-04, and then strengthened the electronic legal environment through Law No. 15-04 regarding electronic signature and authentication.

The issuance of Law No. 25-14 of 2025 represents a new legislative stage in the field of criminal procedures, as it comprehensively reorganized the procedural system, and became the basic legal framework in the light of which modern criminal procedures must be read.⁸

However, legislative development does not mean the end of all problems. Digital evidence is characterized by continuous development, while some technical issues may require more detailed rules, especially with regard to:

- Chain of custody for digital evidence;
- Digital copy safety standards;
- Save metadata;
- cloud computing;
- artificial intelligence;
- Evidence generated by digital platforms;
- Check for fake or modified content with artificial intelligence;
- Limiting liability for digital accounts;
- Evidence extracted from encrypted devices.

Hence, legislation should remain able to evolve in line with technical development.⁹

Conclusion

The digital transformation has reshaped the concept of criminal evidence. Evidence is no longer linked to traditional physical traces only. Rather, it has become possible for the criminal truth to be embodied in intangible digital data, capable of being copied, modified, moved, and deleted, but at the same time capable of providing accurate information about the crime and its perpetrators.

The Algerian legislator has tried to keep pace with these transformations by building a gradual legal system. It began with developing the rules of criminal procedures and special research and investigation methods, then came the provisions of Law No. 09-04 relating to crimes related to media and communication technologies, along with Law No. 15-04 relating

to electronic signature and authentication, leading to Law No. 25-14 containing the Code of Criminal Procedure, which represents the new Algerian procedural framework.

An analysis of this system reveals that the problem no longer lies only in recognizing digital evidence, but rather in ensuring the legality of obtaining it, its integrity, its attribution to its owner, and the possibility of discussing it before the judiciary.

Digital evidence, no matter how technical it is, cannot have absolute value if it was obtained illegally, its safety guarantees are not available, or its relationship with the accused cannot be proven.

The criminal judge's authority to evaluate evidence remains essential, as he must balance the technical value of the evidence with the legal guarantees that govern criminal proof, and base his conviction on legitimate and debatable evidence.

Based on this, the following conclusions can be drawn:

1. Digital evidence has become an essential component of modern forensic evidence.
2. The importance of digital evidence is not limited to cybercrimes, but it can be used in various crimes.
3. Digital evidence is characterized by technical specificity that imposes special rules for its collection, preservation and analysis.
4. The Algerian legislator adopted several texts to keep pace with technological development in the field of proof.
5. Law No. 25-14 containing the Code of Criminal Procedure represents the new procedural framework of the Algerian penal system.
6. The legitimacy of the existence of digital evidence is not enough, but its integrity, authenticity, and attribution must be verified.
7. Technical expertise has become an important element in interpreting digital evidence.
8. The use of technical means must not lead to unjustified infringement of privacy and confidentiality of communications.
9. The principle of the presumption of innocence and the rights of defense continue to govern the use of digital evidence.
10. Algeria needs more specialization and training in the field of digital forensic investigation.

Recommendations

In light of the previous results, the following recommendations can be made:

First: The need to continue updating procedural legislation in line with rapid technical developments.

Second: Establishing precise and detailed procedural rules regarding collecting, preserving, transferring, and presenting digital evidence before the judiciary.

Third: Adopting unified national protocols for the chain of custody of digital evidence.

Fourth: Strengthening the training of judges, prosecutors, judicial police officers, and lawyers in the field of digital evidence.

Fifth: Supporting specialized laboratories and expertise in digital criminal investigation.

Sixth: Strengthening international judicial cooperation mechanisms to obtain cross-border digital evidence.

Seventh: Achieving a careful balance between the requirements of combating digital crime and protecting private life, confidentiality of communications, and defense rights.

Eighth: Developing future rules for dealing with evidence generated by artificial intelligence and deep fakes, given the new challenges they will pose to the criminal judiciary.

In conclusion, the success of criminal proof in the era of digital transformation does not depend on the state's ability to access data, but rather is linked to its ability to access it in a legitimate manner, preserve it properly, verify its authenticity, enable the defense to discuss it, and ultimately subject it to judicial discretion. Thus, digital transformation becomes a tool for developing criminal justice, not a means for undermining its guarantees.

List of sources and references

First : Legal texts

1. The People's Democratic Republic of Algeria, Law No. 25-14 of 9 Safar 1447 corresponding to August 3, 2025, containing the Code of Criminal Procedure, Official Gazette of the Republic of Algeria, No. 54, year 2025. This law has become the new basic reference in the field of Algerian criminal procedures.
2. People's Democratic Republic of Algeria, Law No. 09-04 of Shaaban 14, 1430 corresponding to August 5, 2009, containing the special rules for preventing and combating crimes related to information and communication technologies, Official Gazette, No. 47, 2009.
3. People's Democratic Republic of Algeria, Law No. 15-04 of February 1, 2015, which establishes the general rules related to electronic signature and authentication, Official Gazette, No. 06, 2015.
4. People's Democratic Republic of Algeria, Law No. 18-05 relating to electronic commerce, Official Gazette of the Republic of Algeria.
5. People's Democratic Republic of Algeria, Law No. 06-01 on the Prevention and Combat of Corruption, amended and supplemented.

Second : Books and references

1. Abdullah Ouhaibia, Explanation of the Algerian Code of Criminal Procedure: Investigation and Investigation, Dar Houma, Algeria.
2. Abdel Aziz Saad, Principles of Procedure before the Criminal Court, Dar Houma, Algeria.
3. Youssef Manasra, Electronic Evidence in Criminal Law: The Path to Transforming Evidence in Criminal Matters - A Comparative Study, Dar Al-Khaldounia, Algeria, 2021, 550 pages.
4. Hussein Taheri, Electronic crimes: their nature, characteristics, classification, prevention, proof and combat, Dar Al-Khaldounia, Algeria, 2022.
5. Khaled Al-Hamad, Massara, Digital Evidence and its Quality Standards in Criminal Evidence, Academic Book Center, Jordan, 2014.

Third : Scientific studies and articles

6. Ayachi Hafidh, The authority of the criminal judge to evaluate electronic evidence according to Algerian legislation, Journal of Law and Political Science, Volume 9, Issue 1, 2023, pp. 551-566.

7. Taboub Fatima Al-Zahra, Electronic signature and authentication under Law No. 15-04 of February 1, 2015, *Annals of the University of Algiers*, Volume 29, Issue 2, 2016, pp. 311-328.
8. Benyamina Amina, New Procedures for Dealing with Proceeds of Crime under the New Code of Criminal Procedure 25-14, *Journal of Judicial Jurisprudence*, Volume 18, Issue 1, 2026, pp. 147-160.
9. Mirawi Abdel Qader, Muwafaq Tariq, The Innovator in Cybercrime under the Procedural Law No. 25-14 and the Penal Code, University of Oran 1, 2026.
10. Belkaoui Naima, Electronic Guide to Algerian Legislation, Ammar Thlidji University in Laghouat, 2024.
11. Nabti Meryem, Investigation by Modern Electronic Means, University of Kasdi-Merbah Ouargla, 2026.
12. Talib Siham, Meliani Abderrahmane Hamid, The legal status of the judicial police and its authority in accordance with the provisions of Law 25-14, Ammar Thilighi University in Laghouat, 2026.
13. Tabakh Hajar, Maklati Sabrina, digital evidence and its role in criminal proof, Mohamed Bashir Brahimi University, Bordj Bou Arreridj, 2024.
14. Dahmani Samir, The prescribed electronic signature - a comparative study between European Directive No. 99/93 and Law No. 15-04, *Journal of Humanities*, Volume 1, Issue 1, 2017, pp. 179-191.

Bibliography

¹ Ayachi Hafidah, The authority of the criminal judge to evaluate electronic evidence according to Algerian legislation, *Journal of Law and Political Science*, Volume 9, Issue 1, 2023, pp. 551-566.

² People's Democratic Republic of Algeria, Law No. 09-04 of Shaaban 14, 1430 corresponding to August 5, 2009, containing special rules for preventing and combating crimes related to information and communication technologies, *Official Gazette of the Republic of Algeria*, No. 47, 2009.

³ Youssef Manasra, *Electronic Evidence in Criminal Law: The Path to Transforming Evidence in Criminal Matters - A Comparative Study*, Dar Al-Khaldounia, Algeria, 2021, 550 pages.

⁴ Nabti Mariam, Investigation by Modern Electronic Means, University of Kasdi-Merbah Ouargla, 2026, p. 25.

⁵ Tabakh Hajar, Maklati Sabrina, Digital Evidence and its Role in Criminal Proof, Mohamed Bashir Brahimi University, Bordj Bou Arreridj, 2024, p. 68.

⁶ Hussein Taheri, Electronic crimes: their nature, characteristics, classification, prevention, proof and combat, Dar Al-Khaldounia, Algeria, 2022, p. 73.

⁷ People's Democratic Republic of Algeria, Law No. 18-05 relating to electronic commerce, *Official Gazette of the Republic of Algeria*.

⁸ Taboub Fatima Al-Zahra, Electronic signature and authentication under Law No. 15-04 of February 1, 2015, *Annals of the University of Algiers*, Volume 29, Issue 2, 2016, pp. 311-328.

⁹ People's Democratic Republic of Algeria, Law No. 06-01 on the Prevention and Combat of Corruption, amended and supplemented.