

Digital Evidence as a Tool for Supporting Justice and Achieving Fairness in the Age of Artificial Intelligence

الدليل الرقمي كأداة لدعم العدالة وتحقيق الإنصاف في عصر الذكاء الاصطناعي

BENGUETTAT Khadidja*

Faculty of Law and Political Science University of Mostaganem (Algeria)

Laboratory of International Law for Sustainable Development

khadidja.benguettat@univ-mosta.dz

Date of Submission 02-04-2026 Date of Final Acceptance 08-06-2026 Date of Publication June 2026

Abstract:

Technological advancements have made digital evidence a cornerstone of modern justice, especially with the rise of cybercrimes. This study examines how digital evidence enhances judicial efficiency by providing accurate, reliable data for decision-making. It further explores the role of Artificial Intelligence in analyzing evidence to detect patterns and forgery, significantly increasing judicial speed. However, the transition presents legal challenges regarding admissibility and ethical concerns over data privacy. The research aims to provide a comprehensive vision for utilizing digital evidence to achieve transparency and efficiency. Ultimately, it emphasizes the need for robust legal safeguards to protect individual rights in the AI era. This balance ensures that digital tools support justice without compromising fundamental ethical and legal principles.

Keywords : Key Digital Evidence ; Justice; Artificial Intelligence; Electronic Evidence ;Cybercrime.

ملخص:

أحدثت الطفرة التكنولوجية تحولاً جذرياً بجعل الدليل الرقمي حجر الزاوية في العدالة الحديثة، خاصة مع تصاعد الجرائم السيبرانية. تبحث هذه الدراسة في كيفية تعزيز كفاءة الأداء القضائي عبر تقديم بيانات دقيقة وموثوقة تدعم اتخاذ القرار. كما تسلط الضوء على دور تقنيات الذكاء الاصطناعي في تحليل الأدلة واستكشاف الأنماط الإجرامية وكشف التزوير، مما يرفع من سرعة الفصل في القضايا. ومع ذلك، يواجه القضاء تحديات قانونية تتعلق بمدى حجية وقبول هذه الأدلة، وأخرى أخلاقية تخص حماية الخصوصية. تسعى الدراسة لتقديم رؤية شاملة لتوظيف الدليل الرقمي كأداة فعالة لتحقيق الشفافية والنجاعة القضائية. وفي الختام، تؤكد الدراسة على ضرورة وجود ضمانات قانونية صارمة تحمي حقوق الأفراد في عصر الذكاء الاصطناعي، لضمان توازن دقيق بين الاستفادة من التطور التقني والالتزام بالمبادئ الأخلاقية والقانونية.

الكلمات المفتاحية: الدليل الرقمي ؛ العدالة؛ الذكاء الاصطناعي ؛ الإثبات الإلكتروني ؛ الجرائم السيبرانية.

* Corresponding Author: BENGUETTAT Khadidja

Introduction

With the rapid technological advancement of and the widespread use of artificial intelligence applications in multiple domains of life, the world has witnessed a qualitative transformation in the ways crimes are committed and in the methods of criminal investigation. Crimes are no longer committed through simple traditional means; rather, the extensive use of digital media and electronic communications has become a new factor in the criminal landscape. This development has necessitates the creation of modern evidentiary tools capable of keeping pace with these transformations. In this context, digital evidence has appeared as a fundamental tool for supporting justice and fulfilling fairness, as it enables the judiciary to uncover the factual truth and identify responsibility with greater accuracy through the analysis of data stored on computers, digital networks, and electronic communication devices.

In addition to its significance in criminal proof, digital evidence raises fundamental challenges, particularly with regard to the right to privacy and the protection of personal information. This is due to the dynamic and mobile nature of digital data, as well as the potential implications of electronic surveillance for individual rights. The balance between the need for criminal proof and the protection of fundamental rights constitutes the central focus of this study and highlights the significance of examining how digital evidence can be used in a manner that achieves justice without infringing upon individual rights.

The objectives of this study are to clarify the nature of digital evidence and its distinctive features compared with traditional criminal evidence, and to analyze the role of digital evidence in supporting justice and achieving fairness in criminal cases. The research also aims to highlight the legal and ethical challenges related to the use of digital evidence, particularly with regard to informational privacy, and to propose recommendations to ensure that digital evidence is employed in a manner consistent with the principles of justice and human rights.

This research paper centered on the following problem statement: **How can digital evidence serve as an effective tool for supporting justice and achieving fairness while preserving the fundamental rights and freedoms of individuals in the age of artificial intelligence?**

This research adopted a comparative analytical approach by examining digital evidence across various legal systems and reviewing the opinions of legal scholars concerning its significance and legal nature. It also used the descriptive method to clarify the features of digital evidence and the methods of its use in criminal proof, in addition to an applied analytical approach through the examination of judicial cases associated with the use of digital evidence.

Based on the above, the study is divided into two chapters. The first chapter addresses the concept of digital evidence within the framework of contemporary criminal evidence, while the second chapter examines the impact of digital evidence on informational privacy.

Section I: The Concept of Digital Evidence within the Framework of Contemporary Criminal Evidence

Evidence constitutes the essence of criminal proof in all situations associated with establishing any fact of a criminal nature. Criminal proof is referred to as “everything that leads to the revelation of the truth in order to judge the accused in criminal matters; namely, to establish the occurrence of the crime and attribute its commission to the accused.”¹ On the other hand, criminal evidence is defined as “the evidentiary means itself employed to establish certainty in the mind of the judge or to give greater weight to a position of doubt.”² Therefore, criminal evidence represents the primary means relied upon to uncover the criminal truth, whether to prove the commission of the crime and attribute

it to the accused or to refute such attribution. The criminal judge relies on this evidence to form his or her conviction and to render a judicial ruling, which ultimately determines the fate of the accused either conviction or acquittal. However, the tremendous technological development witnessed globally, particularly in communications and information technology, has given rise to new forms of crime known as cybercrimes. It has also transformed the nature and methods of committing traditional crimes, which are now conducted through advanced technological means and at unprecedented speed. In light of this transformation, a new type of criminal evidence has emerged, known as “digital evidence” or “electronic evidence,” which has become one of the most significant modern tools in the field of criminal proof³.

A) Definition and Legal Nature of Digital Evidence

The terminological definitions of the concept of digital evidence have varied; however, they all converge on a common essence, namely its connection to the electronic environment in which it originates and from which it is derived. This type of evidence possesses unique features that distinguish it from traditional criminal evidence, both in terms of its intangible nature and the methods utilized for its collection, preservation, and analysis.

1- Definition of Digital Evidence

Digital evidence is referred to as “evidence that has its basis in the virtual world and leads to the crime, or information that is accepted by logic and reason and supported by science, obtained through legal and scientific procedures through the translation of computational data stored in computer systems, their accessories, and communication networks. It can be employed at any phase of the investigation or trial to establish the truth of an act or a matter related to a crime or the victim.”⁴

It is also defined as “evidence obtained from computer devices in the form of magnetic or electrical waves and pulses that can be collected and analyzed through specialized application programs and technological tools. It represents a digital element capable of providing information in multiple forms, such as written texts, images, sounds, or graphics, for the purpose of being relied upon by law enforcement authorities.”⁵ Therefore, digital evidence may be referred as a set of data or information of an electronic nature that is stored, processed, or transmitted through computer systems or digital media. It exists within the virtual environment and is employed to detect crimes or to establish the link between a crime and its perpetrator.

2- Distinctive Characteristics of Digital Evidence

Digital evidence possesses a set of characteristics that distinguish it from other forms of criminal evidence, including the following:

- **Digital Evidence as Scientific and Technical Evidence:**

Digital evidence essentially consists of data and information of an electronic and intangible nature, which are accessed and processed through computer devices and equipment, relying on specialized software and computer systems. This makes it one of the modern scientific and technical forms of evidence, due to its close link with the digital and virtual environment. Furthermore, since digital evidence exists as digital pulses of a dynamic nature marked by extremely high speed and the ability to transcend the limits of time and space, it is fundamentally technology-based and depends on modern techniques throughout all phases of collection, analysis, and use as evidence⁶.

- **The Evolving Nature of Digital Evidence:**

Digital evidence is inherently considered an evolving form of evidence, as it possesses the capacity to develop continuously in line with the ongoing advancement of the digital environment, which is fundamentally grounded in the constant renewal and updating of technologies and information systems⁷.

- **The Difficulty of Destroying Digital Evidence:**

Digital evidence may be subject to total or partial destruction due to deletion or erasure. However, this does not necessarily result in its permanent loss, as in many cases its content can be recovered from computer memory or through reliance on backup copies stored within digital systems⁸.

3- Main Categories of Digital Evidence in Cybercrime

Most criminal law scholars have not addressed digital criminal evidence in a comprehensive or detailed manner, due to the novelty of this type of evidence and its specific nature, which is closely related to a technological environment distinguished by continuous development and rapid change⁹. However, there have been scholarly attempts to categorize digital evidence as follows:

- **Digital evidence associated with computer devices and networks:** This involves evidence extracted from computer outputs, software, and the digital data or files they contain.
- **Digital evidence related to the Internet:** This includes any data or digital traces resulting from the utilization of the World Wide Web.
- **Digital evidence linked to information exchange protocols between devices on global networks:** These are evidentiary components derived from data exchange operations between devices over multiple networks.
- **Digital evidence related to the World Wide Web environment:** This encompasses data and digital traces generated from interactions within the web environment, whether on websites or on various digital platforms¹⁰.

B) Procedures for Collecting Digital Evidence and the Criminal Judge's Assessment of Its Evidentiary Value

Obtaining digital evidence necessitates following a set of specific procedures. As a type of criminal evidence, it is subject to examination and verification like any other form of evidence, and its strength and value are evaluated by the criminal judge.

1- Legal Procedures for Collecting Digital Evidence

The procedures for obtaining digital evidence can be divided into two categories: traditional procedures and modern procedures, each of which will be addressed in detail below.

- **Traditional Methods of Collecting Digital Evidence**

Traditional procedures for gathering digital evidence focus on inspection, search, and seizure.

- Inspection in the Digital Environment

Inspection is referred to as: “observing the place, the suspect, or any object in order to establish its condition and secure everything necessary to uncover the truth.”¹¹ Technical inspection in the digital environment is carried out by judicial police officers at the location where the digital evidence is found, usually a computer and the digital data stored in its memory. This process is conducted with the assistance of specialists and experts in information technology to ensure proper handling of devices and data, thereby preserving both the integrity and accuracy of the digital evidence.

- Search in the Digital Environment

The search procedure is an investigative measure aimed at uncovering the truth¹² within private repositories. Its purpose is to access evidence that significantly contributes to revealing and establishing the facts. In the digital environment, the scope of a search encompasses the computer, the server, and multiple associated technical peripherals, as all of these components may contain data or information relevant to digital evidence¹³.

- Seizure Procedure

Seizure in the digital environment concerns components of an intangible nature, such as data, electronic correspondence, and communications. The issue of seizing these elements has generated extensive scholarly debate and legislative divergence among legal systems concerning the legality and feasibility of seizing electronic data, given its unique intangible nature¹⁴.

• Modern Procedures for Obtaining Digital Evidence

In line with rapid technological developments, comparative criminal procedural laws have adopted modern procedures tailored to the specific nature of the digital environment. Due to the fast-changing and dynamic nature of electronic data, it has become necessary to develop effective legal mechanisms to ensure the collection and preservation of digital evidence before it is lost or altered. This is reflected in the adoption of two primary procedures: urgent preservation of stored data and interception of electronic communications, which represent the most notable advancements in the domain of obtaining digital evidence. Each will be addressed in detail below.

- Urgent Preservation of Stored Data

Urgent preservation of stored data is defined as: “the element authority directing service providers to preserve information stored in their possession or under their control pending the adoption of other legal measures, such as a search or an order to submit the stored information.”¹⁵

This procedure applies to previously gathered and retained stored data held by custodians, such as telecommunications or Internet service providers. It is regarded as a modern means of securing digital evidence due to the high susceptibility of electronic data to alteration or destruction, which could compromise its evidentiary value. Therefore, urgent preservation serves both as a method for obtaining digital evidence and as a significant tool for protecting the integrity of electronic data contained in the evidence before it is lost or tampered with¹⁶ (Charaf Eddine, 2018, p. 182).

- Interception of Electronic Communications

Stored electronic communications are regarded as passive data. They include exchanges via email, unopened voice messages at the service provider, and other electronic correspondence. The information subject to interception mainly concerns transmission data, namely, data processed by

information systems that handle communications as they pass through the network. This system constitutes a fundamental component in the chain of electronic communications¹⁷.

Algerian legislation has attempted to establish a legal framework for collecting digital evidence through Law No. 09-04 relating to the prevention and combating of crimes associated with information and communication technologies. This law grants judicial authorities the power to implement technical mechanisms for monitoring electronic communications and conducting searches within information systems. However, despite this legislative effort, the Algerian legal framework still faces practical and technical challenges concerning the admissibility, integrity, and authenticity of digital evidence, particularly in cases involving advanced artificial intelligence technologies.

2- Judicial Evaluation of the Evidentiary Value of Digital Evidence

The primary objective of criminal evidence is to ascertain the factual truth concerning criminal events that occurred in the external world, and to identify both their occurrence and attribution to a specific actor. Since the criminal judge has the authority to assess the evidence presented before them to reach this truth, this authority is closely related to the principle of judicial conviction, one of the most fundamental principles underpinning the criminal evidence system. Judicial conviction entails that the judge forms their belief grounded in sufficient and persuasive evidence available before them, allowing them to reason their judgment, whether by establishing the facts or negating them, and by attributing them to the accused or absolving him therefrom¹⁸.

The application of the principle of judicial conviction results in two fundamental outcomes: the judge's freedom to admit evidence and the judge's freedom to assess it¹⁹. However, this freedom is not absolute; no evidence can be assessed unless the criminal judge first verifies its legality²⁰. The legality of criminal evidence refers to obtaining it through proper legal procedures that align with statutory rules, ensuring the protection of fundamental individual rights and forming one of the essential pillars of a fair criminal trial.

The assessment of digital evidence by the criminal judge is governed by the principles of discretion and judicial conviction. However, this freedom is not unrestricted but constrained by a set of fundamental rules. The process of assessment and conviction requires that the evidence be presented for discussion before the court, whether by the public prosecutor, the trial judge, or the parties and their representatives, and that the evidence be available in its original form within the criminal case file. The court may also rely on experts in information systems to examine and discuss digital evidence, meaning that this type of evidence, like other forms of criminal evidence, is subject to legal discussion before being relied upon for proof²¹. Given the significance of examining the evidence to allow the parties to exercise their guaranteed right of defense²², the criminal judge possesses the authority to admit or exclude digital evidence when forming their conviction, according to what they find convincing and reassuring to their conscience. In light of this liability, it is necessary to place greater emphasis on the knowledge and training of criminal judges in digital evidence and modern technological environments, enabling them to acquire sufficient expertise that directly influences the processes of assessment and judicial conviction during case adjudication.

The Algerian criminal justice system grants judges discretionary authority in assessing criminal evidence, including digital evidence, in accordance with the principle of judicial conviction. Nevertheless, the technical complexity of digital evidence requires specialized expertise in cybersecurity, digital forensics, and artificial intelligence tools. This creates an urgent need for continuous judicial training to ensure that judges are capable of understanding the technical dimensions of digital evidence and evaluating its reliability without compromising the guarantees of a fair trial.

Section II: The Impact of Digital Evidence on Information Privacy

An individual's private life constitutes an essential and fundamental component that must not be violated under any circumstances, even incidentally. Private life represents the repository of an individual's secrets and forms an inseparable part of their personality and existence. Given the importance of this right, Islamic law has afforded special protection to human life and dignity, even preceding positive legislation in highlighting this right. Similarly, multiple civil legislations have placed significant importance on private life, recognizing it as a right for every individual, whether a natural or legal person, and have made respect for this right, and the prohibition of encroachment upon it, a legal obligation, thereby ensuring the protection of human beings and the preservation of their private lives. Article 46 thereof provides as follows: "The sanctity of a citizen's private life and honor shall not be violated, and it is safeguarded by law. The confidentiality of all forms of private correspondence and communication is guaranteed..."²³

With the technological development of communication tools, individuals increasingly share information about their lives through the digital space. Such information falls within the scope of the right to privacy. Notably, the Algerian legislator, recognizing the significance of personal information, enacted Law No. 18/07, which provides special protection for individuals in the processing of personal data²⁴.

A) The Legal Framework of the Right to Digital Privacy

In the era of information and communication technology, personal data are increasingly gathered and analyzed over the Internet. This digital transformation raises questions about how to safeguard individuals from the misuse of their personal information.

This protection is defined to as "digital privacy", which is the right of individuals to control their personal information while utilizing technology. Digital privacy involves safeguarding data from unauthorized access and ensuring it is not used for unlawful purposes.

1- Definition and Scope of Digital Privacy

This right has been discussed through multiple scholarly and legal definitions, as outlined below.

- **Definition of the Right to Digital Privacy**

The scholar Alan Weston defined this right as the right of individuals to determine when, how, and to what extent information about them is disclosed to others. Miller described it as the ability of individuals to control the flow of information concerning themselves²⁵. Ruth Gavison referred to it based on three components: secrecy, solitude, and anonymity and considered it the right to protection against interference in private life and family affairs, whether through direct physical means or through the spread of information.

Hence, digital privacy can be defined as all personal data of an individual utilized in physical or digital spaces that require protection from risks, breaches, or unauthorized access²⁶.

- **Legal Definition of the Right to Digital Privacy**

International and national legal instruments have placed considerable emphasis on this right. For instance, the Universal Declaration of Human Rights (1948) enshrines its protection. Article 12 states: "No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence, nor to attacks on his honor and reputation. Everyone has the right to the protection

of the law against such interference or attacks." The UN General Assembly has further highlighted the protection and promotion of the right to privacy online to the same extent as offline, urging states to respect and protect this right in light of technological developments. In this context, it issued a special report on safeguarding individual privacy concerning electronic surveillance, interception of digital communications, and all personal data under Resolution No. 68-167²⁷.

The right to privacy is also safeguarded under the European Convention on Human Rights and Fundamental Freedoms. In France, Law No. 78-17 of 6 January 1978, regarding information technology, files, and freedoms, established fundamental principles for handling and processing personal data. This was later supplemented by the Digital Economy Confidence Law of 2004.

In Algeria, the Constitution, alongside safeguarding the right to privacy, also affirms the protection of personal data. This was formalized in the 2016 constitutional amendment, reaffirmed in 2020, by virtue of Article 47 thereof, paragraph 4, which states: "**The protection of natural persons in the processing of personal data is a fundamental right**"²⁸.

Following this constitutional guarantee, the legislator, approximately two years after the amendment, enacted Law 18-07, regarding the protection of natural persons concerning personal data. This law provided a significant legislative framework at a time when technological and digital developments were rapidly expanding in all sectors, particularly facilitating the exchange of personal information via social media platforms and multiple Internet sites²⁹.

Therefore, the term digital privacy refers to the scope of an individual's private life and the degree of control they exercise over personal data employed in multiple transactions, ensuring it is not violated by others through new applications or technologies developed with artificial intelligence³⁰.

The Algerian legislator reinforced constitutional protection for informational privacy through the constitutional amendments and further strengthened this protection under Law No. 18-07 concerning the protection of natural persons in the processing of personal data. This law represents an important legislative step toward regulating the collection, storage, and processing of personal data in the digital environment. However, the rapid evolution of artificial intelligence applications raises new legal concerns regarding automated data analysis and algorithmic surveillance, which may exceed the traditional safeguards established by current legislation.

2- Components of the Right to Digital Privacy

The scope of the right to privacy in the context of smart technologies differs from its traditional conception. Personal information and individual secrets, once difficult to access, are now easily transmitted and circulated through various modern technological means. Accordingly, digital privacy includes several interrelated aspects, summarized as follows:

- **Bodily Privacy:** At times, an individual may be subjected to unwanted external interventions that impact the privacy and integrity of their body, such as mandatory vaccinations.
- **Privacy of Personal Behaviour:** This encompasses an individual's ability to act freely without unwanted monitoring or interference, covering religious, political, and other personal activities.
- **Privacy of Personal Communications:** This refers to an individual's freedom to communicate utilizing multiple technological means without their communications being monitored or intercepted by others.

- **Privacy of Personal Data:** Also referred to as information privacy, this involves an individual's right to control the flow of their data and information, whether private and unknown to others, or shared confidentially with a select group. According to the European General Data Protection Regulation (GDPR), personal data includes any information relating to an identified or identifiable natural person, directly or indirectly, such as addresses, photographs, religious beliefs, and other data related to a specific individual's identity.

B) The Impact of Digital Evidence on Informational Privacy

The critical significance of digital evidence in criminal investigations cannot be denied. However, its use may potentially infringe on informational privacy, as it is often associated with electronic monitoring, which can violate individuals' rights to privacy³¹. The risk of infringement increases when monitoring produces negative outcomes, such as accessing a suspect's email only to later find that they have no connection to the crime. Despite this conflict, the requirements of criminal evidence and the necessity of fighting crime, particularly crimes impacting state or public security, justify the use of such evidence. Therefore, infringements on informational privacy mainly occur through electronic surveillance procedures used to obtain digital evidence. This emphasizes the need to address the concepts of electronic surveillance and the monitoring of electronic communications.

1- Electronic Surveillance as a Means of Obtaining Digital Evidence

- **Electronic surveillance, or Keepwatch,** is defined as:

"Monitoring an electronic communications network or the activity conducted by a monitor employing electronic technology to collect data and information about a suspect or something related to time (i.e., date and time) for a security purpose or any other objective³²."

It is also referred as: "A method of collecting data and information about a suspect by monitoring their electronic communications carried out over the Internet." Furthermore, it has been described as: "The act of eavesdropping and recording private conversations, whether direct or indirect, namely, face-to-face exchanges or communications conducted through wired or wireless means."³³ Electronic surveillance typically includes monitoring the following:

- **Electronic Mail (Email):**

Email is one of the most commonly used forms of electronic communication. It consists of two main elements: the header and the body. The header contains essential information about the sender and recipient, as well as routing data to ensure delivery to the correct address. The body includes the actual content of the message as written by the sender. When a message is sent, it travels from the sender's computer via a telephone line to the email server, where it is stored in the sender's mailbox before being delivered to the recipient³⁴.

- **Newsgroups and Chat Rooms:**

A newsgroup refers to public discussion areas on the Internet where users can discuss specific topics and exchange information and images. Chat rooms are well-known online spaces that allow participants to engage in real-time conversations. Each user can send messages that can be read by other members participating in the chat room³⁵.

2- Monitoring Electronic Communications

Article 2, paragraph “W” of Law No. 09/04, which includes special provisions for the prevention and fight of crimes associated with information and communication technology, defines electronic communications as: "Any correspondence, sending, or receiving of signs, signals, writings, images, sounds, or other information by any electronic means.³⁶" Electronic communications also encompass communications carried out via social media networks on the Internet. Social media networks are referred to as: "Interactive networks that enables users to communicate at any time and from any location worldwide. They acquired the name ‘social’ because they promote relationships and connections among people. Recently, their role has expanded beyond social interaction to become a means of expression and protest." Prominent social media networks include Facebook and YouTube.

During the investigation stage, Algerian legislation grants judicial authorities the power to take special measures to uncover the truth. Judicial police officers, the public prosecutor, and investigating judges are authorized to temporarily infringe upon the right to privacy to clarify the circumstances of a crime³⁷. This is achieved through measures introduced in the Code of Criminal Procedure, as well as under Law No. 09-04 regarding special provisions for the prevention and combat of crimes related to information and communication technologies, with electronic surveillance being one of these measures.

The Algerian legislator regulated this procedure under Article 03 of Law No. 09-04 relating to the specific rules for the prevention and combating of crimes linked with information and communication technologies. It provides that: “Subject to the legal provisions guaranteeing the confidentiality of correspondence and communications, and where required for the protection of public order or for the needs of ongoing investigations or judicial inquiries, and in accordance with the rules set out in the Code of Criminal Procedure and in this law, technical arrangements may be implemented to monitor electronic communications and to collect and record their content in real time, as well as to conduct search and seizure procedures within an information system.” As for the cases in which electronic communications may be monitored, they include the following:

- Preventing acts categorized as terrorism, sabotage, or crimes impacting state security.
- When there is information demonstrating a potential attack on an information system that threatens public order, national defense, state institutions, or the national economy.
- Investigative and judicial purposes, when fulfilling the objectives of ongoing investigations is difficult without resorting to electronic surveillance.
- Within the framework of executing international judicial assistance.

Electronic surveillance may only be carried out with written authorization from the competent judicial authority. In cases regarding acts of terrorism, sabotage, or threats to state security, the Public Prosecutor at the Court of Algiers has jurisdiction to authorize it.

The officers authorized to conduct this procedure for crimes of terrorism, sabotage, and threats to state security are members of the National Agency for the Prevention and Combat of Crimes Related to Information and Communication Technologies, organized under Presidential Decree No. 15-261 dated 24 Dhu al-Hijjah 1436 (Presidential Decree 15-261, 2015). Authorization is granted for a period of six months, renewable based on a report detailing the technical arrangements used and their intended purposes.

Although electronic surveillance constitutes an effective mechanism for combating cybercrime and protecting public security, its extensive use may lead to disproportionate interference with individuals' private lives. Algerian legislation therefore attempts to balance security requirements with constitutional guarantees of privacy by subjecting surveillance procedures to judicial authorization and legal oversight. Despite these guarantees, concerns remain regarding the absence of detailed legal provisions regulating the use of artificial intelligence in electronic surveillance operations.

Conclusion:

This study reveals that digital evidence has become a fundamental pillar of the modern criminal evidence system, due to the accuracy and speed it provides in uncovering the truth. It reached the following results:

- The global digital transformation has not only impacted patterns of crime but has also reshaped the rules of criminal evidence. Digital evidence has become a central element in most criminal cases.
- Digital evidence is distinguished by its complex technical nature, which raises legal and ethical challenges that necessitate careful management to maintain a balance between the requirements of justice and the protection of individuals' fundamental rights.
- Technological advancements and artificial intelligence have created a new reality in the domain of evidence, making it essential to revisit traditional legal rules to align with the features of digital evidence.
- The study emphasized specific legal challenges associated with the admissibility of evidence, algorithmic transparency, guarantees of a fair trial, and the protection of privacy. This highlights a clear gap between rapid technological developments and procedural legislative frameworks, which in numerous legal systems remain inadequately equipped to accommodate these changes.

Based on the above, the key recommendations are as follows:

- Developing a dedicated legal framework for digital evidence within national procedural legislation.
- Providing comprehensive training for judges and public prosecutors in digital technologies and cybersecurity.
- Establishing clear regulations for the collection of digital evidence to ensure its legality and protect privacy.
- Strengthening international cooperation in fighting cybercrime and sharing information.
- Implementing effective mechanisms to safeguard personal data and prevent its misuse during investigations.
- Encouraging academic research on the intersection of artificial intelligence and criminal evidence.
- Amending Algerian criminal procedural legislation to establish a comprehensive legal framework governing the use of artificial intelligence technologies in the collection, analysis, and admissibility of digital evidence while ensuring the protection of fundamental rights and informational privacy.

Implementing these measures will help fulfill a genuine balance between the requirements of criminal justice in the digital era and the protection of individuals' fundamental rights and freedoms.

Bibliography:

- Books

- Abdel Kader, Ashraf Kandil, Criminal Evidence in Cybercrime, Dar Al-Jami'a Al-Jadida, Alexandria, 2015.
- Al-Abadi, Mohamed Abdel Karim, The Inner Conviction of the Criminal Judge and Judicial Oversight over It: A Comparative Analytical Study, Dar Al-Fikr, Jordan, 2010.
- Al-Bishri, Hamad Al-Amin, Investigation of Emerging Crimes, Dar Al-Hamed for Publishing and Distribution, Jordan, 2014.
- Al-Fiqi, Fouad, The Inner Conviction of the Criminal Judge in Light of Modern Means of Evidence, Dar Al-Nahda Al-Arabia, Cairo, 2016.
- Al-Mahlawi, Anis Hasib Al-Sayed, The Inner Conviction of the Criminal Judge in Light of Modern Means of Evidence, Dar Al-Fikr Al-Jami'i, Alexandria, 2016.
- Al-Shawabkeh, Mohamed Amine, Computer, Internet, and Cybercrime, Dar Al-Thaqafa for Publishing and Distribution, Jordan, 2009.
- Ben Kara, Aicha, The Evidentiary Value of Electronic Evidence in Criminal Proof, Dar Al-Jami'a Al-Jadida, Egypt, 2010.
- Harwal, Nabila Hiba, Procedural Aspects of Internet Crimes, Dar Al-Fikr Al-Jami'i, Alexandria, 2006.
- Kour, Tarek, Mechanisms for Combating Exchange Crimes in Light of Amendments and Judicial Rulings, Dar Houma, Algeria, 2014.
- Nouh, Luay Abdullah, The Legality of Electronic Surveillance in Criminal Evidence, Arab Studies Center, Egypt, 2018.

B- Theses

- Massaoud, Ahmed Mariam, Mechanisms for Combating Information and Communication Technology Crimes in Light of Law No. 09/04, Master's Thesis, Specialization Law, University of Ouargla, Algeria, 2012/2013.

C- Newspaper Articles

- Ben Salem, Abdallah Widad Chibani, "The Right to Informational Privacy in Light of Artificial Intelligence", Journal of Legal and Economic Studies, University Center Si El-Haouas, Brika, Algeria, Vol. 6, No. 2, 2023.
- Charaf Eddine, Warda, "Procedural Provisions for Combating the Crime of Human Trafficking Committed through Information Technology", Al-Ijtihad Al-Qada'i Journal, University of Biskra, Issue 17, 2018.
- Kahlaoui, Abdelhadi and Ben Zita, Abdelhadi, "Mechanisms for Protecting Personal Data under Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data", Journal of Law and Political Science, University Center Naâma, Vol. 7, No. 2, September 2021.
- Khodja Lakhdar, Idris, "Proof by Digital Criminal Evidence in Light of Algerian Legislation", Afaq Journal for Comparative Legal Studies, University of Saïda, Issue 8, 2017.
- Maazouz, Dalila and Ouali, Nadia, "Risks of Artificial Intelligence on Digital Privacy and Mechanisms for Its Protection", Journal of Legal and Social Sciences, University of Djelfa, Vol. 9, No. 3, September 2018.

- Mahmoudi, Nour El Houda, "The Evidentiary Value of Digital Evidence in Proving Cybercrime", *Al-Bahith Journal for Academic Studies*, University of Batna 1, Issue 11, June 2017.
- Roubah, Ilham Shahrazad, "Digital Evidence between the Legitimacy of Proof and the Violation of Informational Privacy", *Journal of Legal and Political Research and Studies*, University of Blida 2, Vol. 5, No. 2, 2018.

D- Legal Texts (National Legislation)

- Law No. 16-01, Containing the Constitutional Amendment of the Algerian Constitution, *Official Gazette of the Algerian Republic*, No. 14, 2016.
- Law No. 18-07, On the Protection of Natural Persons in the Processing of Personal Data, *Official Gazette of the Algerian Republic*, No. 34, June 10, 2018 (as amended by Law 25-11, 2025).
- Law No. 09/04, On Specific Rules for the Prevention and Combating of Crimes Related to Information and Communication Technologies, *Official Gazette of the Algerian Republic*, No. 47, Algeria, 2009.

Citations:

¹ Abdel Halim Fouad Al-Fiqi, *The Inner Conviction of the Criminal Judge in Light of Modern Means of Evidence*, Dar Al-Nahda Al-Arabia, Cairo, 2016, p. 1.

² Mohamed Abdel Karim Al-Abadi, *The Inner Conviction of the Criminal Judge and Judicial Oversight over It: A Comparative Analytical Study*, Dar Al-Fikr, Jordan, 2010, p. 67.

³ Aicha Ben Kara, *The Evidentiary Value of Electronic Evidence in Criminal Proof*, Dar Al-Jami'a Al-Jadida, Egypt, 2010, p. 23.

⁴ Ashraf Kandil Abdel Kader, *Criminal Evidence in Cybercrime*, Dar Al-Jami'a Al-Jadida, Alexandria, 2015, pp. 123–124.

⁵ Nour El Houda Mahmoudi, *The Evidentiary Value of Digital Evidence in Proving Cybercrime*, *Al-Bahith Journal for Academic Studies*, University of Batna 1, Issue 11, June 2017, p. 911.

⁶ Ashraf Kandil Abdel Kader, *op. cit.*, p. 126.

⁷ Idris Khodja Lakhdar, *Proof by Digital Criminal Evidence in Light of Algerian Legislation*, *Afaq Journal for Comparative Legal Studies*, Issue 8, University of Saida, 2017, p. 157.

⁸ Hamad Al-Amin Al-Bishri, *Investigation of Emerging Crimes*, Dar Al-Hamed for Publishing and Distribution, Jordan, 2014, p. 230.

⁹ Aicha Ben Kara, *op. cit.*, p. 71.

¹⁰ Idris Khodja Lakhdar, *op. cit.*, p. 154.

¹¹ Ashraf Kandil Abdel Kader, *op. cit.*, p. 135.

¹² Ashraf Qandil Abdel Qader, *op. cit.*, p. 87.

¹³ *Ibid.*, p. 149.

¹⁴ Aicha Ben Kara, *op. cit.*, p. 114.

¹⁵ Ashraf Kandil Abdel Kader, *op. cit.*, p. 180.

¹⁶ Warda Charaf Eddine, *Procedural Provisions for Combating the Crime of Human Trafficking Committed through Information Technology*, *Al-Ijtihad Al-Qada'i Journal*, Issue 17, University of Biskra, 2018, p. 182.

¹⁷ Warda Charaf Eddine, *Ibid.*, p. 184.

¹⁸ Anis Hasib Al-Sayed Al-Mahlawi, *The Inner Conviction of the Criminal Judge in Light of Modern Means of Evidence*, *Dar Al-Fikr Al-Jami'i*, Alexandria, 2016, p. 16.

¹⁹ Ashraf Qandil Abdel Qader, *op. cit.*, p. 220.

²⁰ Aisha Ben Kara, *op. cit.*, p. 195.

²¹ Luay Abdullah Nouh, *The Legality of Electronic Surveillance in Criminal Evidence*, Arab Studies Center, Egypt, 2018, p. 54.

²² Mohamed Abdel Karim Al-Abadi, *op. cit.*, p. 178.

²³ Law No. 16-01, Containing the Constitutional Amendment of the Algerian Constitution, Official Gazette of the Algerian Republic, No. 14, 2016, p. 11.

²⁴ Law No. 18-07, dated 25 Ramadan 1439 AH corresponding to 10 June 2018, on the Protection of Natural Persons in the Processing of Personal Data, Official Gazette of the Algerian Republic, No. 34, issued on 10 June 2018, as amended by Law 25-11 in 2025.

²⁵ Abdallah Widad Chibani Ben Salem, *The Right to Informational Privacy in Light of Artificial Intelligence*, Journal of Legal and Economic Studies, Vol. 6, No. 2, University Center Si El-Haouas, Brika, Algeria, 2023, p. 461.

²⁶ Dalila Maazouz, Nadia Ouali, *Risks of Artificial Intelligence on Digital Privacy and Mechanisms for Its Protection*, Journal of Legal and Social Sciences, Vol. 9, No. 3, University of Djelfa, September 2018, p. 818.

²⁷ Abdallah Widad Chibani Ben Salem, *op. cit.*, p. 465.

²⁸ Law 16-01, containing the aforementioned constitutional amendment.

²⁹ Abdelhadi Kahlaoui, Abdelhadi Ben Zita, *Mechanisms for Protecting Personal Data under Law No. 18-07 on the Protection of Natural Persons in the Processing of Personal Data*, Journal of Law and Political Science, Vol. 7, No. 2, University Center Naâma, September 2021, p. 125.

³⁰ Dalila Maazouz, Nadia Ouali, *op. cit.*, p. 819.

³¹ Ilham Shahrazad Roubah, *Digital Evidence between the Legitimacy of Proof and the Violation of Informational Privacy*, Journal of Legal and Political Research and Studies, Vol. 5, No. 2, University of Blida 2, 2018, p. 194.

³² Nabila Hiba Harwal, *Procedural Aspects of Internet Crimes*, Dar Al-Fikr Al-Jami'i, Alexandria, 2006, p. 198.

³³ Ahmed Mariam Massaoud, *Mechanisms for Combating Information and Communication Technology Crimes in Light of Law No. 09/04*, Master's Thesis, Specialization Law, University of Ouargla Algeria, 2012/2013, p. 79.

³⁴ Mohamed Amine Al-Shawabkeh, *Computer, Internet, and Cybercrime*, Dar Al-Thaqafa for Publishing and Distribution, Jordan, 2009, p. 32.

³⁵ Mohamed Amine Al-Shawabkeh, *op. cit.*, pp. 42–45.

³⁶ Law No. 09/04, on Specific Rules for the Prevention and Combating of Crimes Related to Information and Communication Technologies, Algeria, issued on 5 August 2009, Official Gazette of the Algerian Republic, No. 47, 16 August 2009, p. 5.

³⁷ Tarek Kour, *Mechanisms for Combating Exchange Crimes in Light of Amendments and Judicial Rulings*, Dar Houma, Algeria, 2014, p. 32.