RESEARCH ARTICLE

The Legal Nature of Digital Evidence in Cybercrime

Zakaria Hadj Moussa
Doctor (PhD)
University of Abou Bekr Belkaid – Tlemcen, Laboratory of Comparative Law
Algeria
zakaria.hadjmoussa@univ-tlemcen.dz

Samia Kissi
Lecturer (A)
University of Abou Bekr Belkaid – Tlemcen, Laboratory of Private Law
Algeria
kissisamia.6@gmail.com

Doi Serial https://doi.org/10.56334/sei/8.5.37

Keywords digital evidence, cybercrime

Abstract

Despite the great development taking place in the technological field and its benefits at the internal and external levels for the countries of the world, it resulted in new distinct methods of committing crimes, which is known as cybercrime, which made most countries, through their internal legislation, seek to keep pace with these developments to combat this criminal phenomenon by developing Mechanisms and means to combat it, especially the new methods of criminal investigation, distinct from the traditional methods of investigation of violence and torture in order to reach the evidence, so the growing scientific revolution has become dependent on technological and digital methods and this technique on the one hand and on the other hand the privacy that characterizes electronic crimes, which is often difficult to monitor and track And then proving it, which is known as digital evidence, where the following problem is raised: What is the privacy of digital evidence in proving cybercrime? In order to answer this problem, we discuss in this intervention two axes to the concept of digital evidence, as well as digital proof mechanisms in cybercrime.

Citation

Zakaria Hadj M., Samia K. (2025). The Legal Nature of Digital Evidence in Cybercrime. *Science, Education and Innovations in the Context of Modern Problems*, 8(5), 372-383; doi:10.56352/sei/8.5.37. https://imcra-az.org/archive/363-science-education-and-innovations-in-the-context-of-modern-problems-issue-5-volviii-2025.html

Received: 11.10.2024	Accepted: 23.02.2025	Published: 10.05.2025 (available online)

Introduction

Crime is a social phenomenon that results from the conflict and divergence of interests among individuals within society at large. Such conflicts often lead to disputes that, in many cases, result in the commission of various criminal behaviors. These behaviors have evolved in tandem with changes in individuals' lifestyles and differ according to the stages of their lives. Consequently, crime has permeated all aspects of human life and continues to change depending on individuals' goals, motives, and social circumstances, which are influenced by time and place.

With the accelerating pace of scientific and technological advancement, and the emergence of cyberspace and

modern means of communication such as fax, the internet, and other forms of electronic communication via satellites, cybercriminals have exploited these developments to commit crimes that are no longer confined within the borders of a single state. These are innovative and unprecedented crimes that exemplify a form of criminal ingenuity, making it difficult to classify them under the traditional criminal descriptions found in national and foreign penal codes.

To combat cybercrime, it has become essential to adopt new methods fundamentally different from those used to combat traditional crime. This necessity arises due to the inadequacy of conventional investigative procedures in keeping up with the evolution of such crimes. Cybercrimes have shifted the locus of criminal activity from a tangible, physical environment to a virtual space, and from physical evidence to digital or electronic evidence that aligns with the environment in which the crimes are committed.

In our current era, many legal systems have come to recognize electronic evidence as a valid and legally admissible form of proof, on par with traditional types of evidence. However, due to its unique nature, electronic evidence raises several issues, particularly given its susceptibility to alteration at any moment. With the press of a single button, such evidence can be erased, destroyed, or manipulated, casting doubt on its reliability. Despite this, such evidence remains indispensable in prosecuting cybercrimes. Nevertheless, its use is restricted by the overarching principle of respecting individuals' informational privacy.

Based on the foregoing, the central research question of this study can be formulated as follows: What is the role of digital evidence in criminal proof, and what is its probative value?

Significance of the Study

The importance of the topic "The Legal Nature of Digital Evidence in Cybercrime" lies in its treatment of a new type of criminal evidence from both technical and legal perspectives. The value of this study stems from its close connection with a new class of crimes that have emerged alongside technological developments—namely, cybercrimes.

This development necessitated the introduction of digital evidence as a response to such crimes. The criminal judiciary has found itself facing this newly developed form of evidence, which imposes new challenges on criminal judges. Furthermore, this topic addresses one of the most widespread scientific tools in criminal evidence—tools that align with the evolving criminal mindset and require the legislature to enact laws suited to this new reality.

Research Methodology

This study adopts a descriptive methodology by providing a detailed account of digital evidence, including its definition, characteristics, and classifications. In addition, an analytical approach is employed to examine the facts, data, and procedural mechanisms required to obtain digital evidence.

Structure of the Study

This topic is addressed by dividing it into two main chapters. The first chapter is titled "The Conceptual Framework of Digital Criminal Evidence," which includes the definition, characteristics, and classifications of digital evidence. The second chapter is titled "Mechanisms of Digital Evidence in Proving Cybercrime," wherein the conditions for its admissibility, methods of obtaining it, and its probative value are discussed. The study concludes with a presentation of the findings and recommendations reached.

Chapter One: The Conceptual Framework of Digital Criminal Evidence

In this chapter, we examine the concept of digital evidence, its characteristics, and its classifications according to their sources.

First: The Concept of Digital Evidence

Evidence plays a pivotal role in the field of criminal proof, as it is the tool upon which the judge bases their verdict in either convicting or acquitting the accused. Understanding the essence of something requires exploring its definition and distinguishing characteristics.

Studying the nature of digital evidence is indispensable for gaining a comprehensive understanding of this type of evidence, particularly due to its novelty in criminal law and its relation to non-physical technological means. Therefore, it is essential to clarify the essence of digital

criminal evidence by defining it linguistically and terminologically, identifying its characteristics and types, and exploring the means by which it is obtained—thus completing our understanding of its nature, and recognizing the methods and procedures used to collect and document it.

In this first chapter, we shall address both the linguistic and terminological definitions of digital criminal evidence as follows:

1. Definition of Digital Evidence

a. Linguistic Definition:

The word "evidence" (in Arabic: دليل) in the Arabic language refers to that which leads to knowledge or discovery. It is said that someone "guided" or "indicated" something. The term also means "proof" or "guide," and its plural is "adillah." In the Qur'anic usage, the term is found in the verse:

"Have you not seen how your Lord extended the shadow, and if He had willed, He could have made it stationary; then We made the sun its guide." (Surat Al-Furqan, verse 45)

b. Terminological Definition:

In legal terminology, evidence is defined as: "That from which the knowledge of another thing necessarily follows." (Abu Al-Qasim, 1993, p. 177). In other words, evidence is that which can lead to the truth (Abu Al-Qasim, 1993, p. 178). Criminal evidence is defined as "proof or a presumption upon which the accuracy of a fact is based" (Al-Bushra, 1995, p. 105). Another definition states that it is "any material or moral fact that contributes to proving the occurrence of a crime, identifying the perpetrator, or establishing that the crime was committed—either directly or indirectly."

Criminal evidence differs from traces of crime in terms of their intrinsic nature. Criminal evidence may be material, such as the presence of the weapon used in the crime, the perpetrator's fingerprints, or their blood at the crime scene. It may also be moral, such as witness testimony or the confession of the accused. By contrast, a trace is always of a material nature and perceptible through the senses.الأكاديمية الترجمة إليك الإنجليزية، باللغة المطلوبة للفقرات الدقيقة القانونية والأسلوبية النحوية الأخطاء من خالية:

(Abdel-Muttalib, 2014–2015, p. 3)

C. Definition of Digital Forensic Evidence

In the absence of a definition of digital forensic evidence by Algerian and French legislators, we will review several definitions proposed by scholars in criminal law. Some have defined it as evidence derived from computers, presented in the form of magnetic or electrical fields or pulses, which can be collected and analyzed using specific technological software and applications, and subsequently presented in a format admissible before the courts (Al-Matloub, 2006, p. 88).

It has also been defined as: "electronic impulses recorded on material media," or as: "evidence obtained through technical electronic methods from computer data, the internet, connected electronic devices, and communication networks, through legal procedures to be presented before the judiciary as digital forensic evidence valid for establishing a crime" (Al-Halabi, 2011, p. 230).

Others define digital forensic evidence as encompassing all digital information and data capable of proving that a crime has been committed, or establishing a link between the crime and the perpetrator, or between the crime and the victim. Digital data consists of numbers that represent various types of information, including text, graphics, maps, audio, or images. It is essentially a set of valuable information or data for investigation purposes, stored or transmitted through an electronic device.

Most of these definitions describe digital forensic evidence in terms of its composition—as magnetic or electrical fields or pulses representing various types of information or data. However, these definitions are sometimes criticized for focusing solely on evidence extracted from computers or the internet (Al-Halabi, 2011, p. 230), whereas digital forensic evidence can also be sourced from smartphones, GPS devices, or any device capable of processing or storing data.

On another note, definitions provided by scientific working groups on digital evidence and international computer evidence organizations have been criticized for failing to clarify what is meant by the binary format of digital forensic evidence and for overlooking the

nature of the data referred to as digital evidence (Onwuadiamu G. (2025).

To address the shortcomings of these previous definitions, we may propose the following comprehensive definition:

"Digital forensic evidence is evidence extracted from computers and their accessories, the internet, or any other device capable of processing or storing data. It consists of magnetic or electrical fields or pulses that can be collected and analyzed through specialized software and applications to produce various forms of information or data that may be relied upon during investigation or trial."

This proposed definition offers a holistic understanding of digital forensic evidence in terms of its sources—not limited to computers—and clarifies its technical and scientific nature, which requires collection and analysis by specialized experts using specific methods and tools, resulting in reliable digital forensic evidence admissible in criminal proceedings.

2. Characteristics of Digital Forensic Evidence

Digital forensic evidence possesses characteristics closely tied to its origin in the virtual environment—represented by computer systems in both their hardware (physical devices and tools) and software (programs and applications). This virtual nature has impacted the characteristics of such evidence, distinguishing it from traditional physical forensic evidence. These characteristics include:

1. Scientific Nature of Digital Forensic Evidence:

Extracting and analyzing digital forensic evidence necessitates non-traditional methods, involving scientific and technical experimentation on computers used in the commission of crimes (Thunayyan, 2012, p. 74). The process of retrieving such evidence must occur within the geography of the virtual system (Geographic Information System) and comply with relevant information technology laws (Younes, 2006, p. 7).

Consequently, access to or retrieval of digital forensic evidence requires scientific tools and methods due to the technical origin of such evidence.

2. Technical Nature of Digital Forensic Evidence:

Given its scientific characteristics, digital forensic evidence must be handled by technicians specialized in forensic science and the virtual environment (Abdel-Muttalib, 2014–2015, p. 8). The technical nature of such evidence necessitates compatibility between the evidence and the digital environment in which it was generated. Unlike conventional tools that might directly indicate the presence of a weapon used in a crime, digital evidence consists of magnetic or electrical pulses that form information, which can only be interpreted by professionals familiar with the technical ecosystem in which the evidence was created.

One consequence of its technical nature is the ability to produce exact replicas of digital forensic evidence, which retain the same scientific value as the original—unlike traditional evidence, where replication typically results in loss of authenticity (Farghali & Mohamed Obeid Saif, 2007, p. 15). This ensures the preservation of the original against loss, alteration, or damage, as the duplication process matches the method of creation.

Furthermore, unlike traditional evidence, digital forensic evidence is difficult to erase permanently. Even if deletion is attempted, it can often be recovered using specialized recovery software. Attempts by the perpetrator to erase such evidence are themselves recorded and may serve as incriminating evidence.

3. Difficulty of Erasing Digital Evidence:

This is one of the most notable characteristics of digital evidence. Traditional evidence, such as written confessions or fingerprints, can be easily destroyed. In contrast, digital evidence, even after deletion or concealment, can often be retrieved, repaired, or uncovered through sophisticated software tools like "Recover Lost Data." These tools can recover deleted or formatted data including text, images, and audio.

Hence, efforts by the perpetrator to hide or delete digital evidence are often futile and may, in fact, create additional evidence against them (Mustafa, 2010, pp. 62–63). The act of deletion itself becomes an evidentiary event, as system logs may record attempts to tamper with or erase data.

This characteristic motivates continued efforts to investigate cybercrimes and emphasizes the need for vigilance. However, the same property also implies vulnerability: digital evidence is inherently fragile and can be

corrupted or lost if not properly handled. Such losses are more indicative of limitations in the technological capabilities of judicial systems than of the evidence's destructibility—underscoring the importance of developing justice system infrastructure and expertise (Ezzat, 2010, pp. 655–656).

4. Diversity and Evolvability of Digital Evidence:

Although digital evidence is unified in its computational and digital nature, it can manifest in various formats. The term "digital evidence" encompasses all types of electronically transmittable data that may bear relevance to a crime, a suspect, or a victim.

This diversity is reflected in its various forms—some digital evidence may appear as unreadable data (e.g., server logs), while others may be comprehensible documents processed using word processing software. It may also appear in the form of still or moving images, audio-visual recordings, or data stored in email systems. Therefore, this characteristic requires legal and technical systems to keep pace with ongoing developments in information technology (Ezzat, 2010, pp. 651–652).

he Reproducibility of Electronic Evidence

Electronic forensic evidence can be duplicated in a manner identical to the original, retaining the same scientific value. This characteristic does not exist in traditional physical evidence, thus providing a highly effective safeguard to preserve evidence from loss, damage, or alteration by creating exact replicas. This principle was enshrined in Belgian Law by the amendment of November 28, 2000, which added Article 39 permitting the seizure of electronic evidence, including copies of materials stored in automated data processing systems, for judicial consideration.

Moreover, electronic evidence is characterized by high storage capacity. A digital video device, for instance, can store hundreds of images, while a small disk can hold the equivalent of a small library. Additionally, electronic evidence has the unique capability to track and analyze information about a suspect in real time. It can record an individual's movements, habits, behaviors, and personal data, thus enabling criminal investigations to reach their conclusions more efficiently than with material evidence (Mustafa, 2010, p. 64).

Accordingly, the aforementioned features grant electronic evidence a distinctive nature, making it the most suitable and reliable means of proving cybercrimes—whether committed through automated data processing systems or targeting those systems.

Third: Classifications of Electronic Evidence

Before discussing the various classifications of electronic evidence, it is important to refer to doctrinal attempts to categorize forensic evidence. Among the most relevant to our study is the classification of evidence according to its source, as this distinction clarifies the difference between traditional forensic evidence and electronic evidence.

1. Classification of Forensic Evidence by Source

a. Legal Evidence:

This refers to evidence types defined by the legislator, along with their probative value in civil matters. In criminal matters, however, the range of admissible evidence is not exhaustively defined, and judges have wide discretion in forming their conviction. Nevertheless, certain exceptions exist where proof or persuasion is subject to restrictions (Mustafa, 2010, p. 66).

b. Technical (Scientific) Evidence:

This type stems from an expert opinion based on scientific standards and typically takes the form of expert analysis or testimony (Ezzat, 2010, p. 609).

c. Testimonial Evidence:

Originates from individuals who have perceived information relevant to the case through one of their senses, such as confessions (Husseini, 2015, p. 155).

d. Physical Evidence:

This is tangible material evidence that speaks for itself and has a direct impact on the judge's conviction (Bouchra, 1995, p. 234).

Doctrinal debate has emerged concerning where electronic evidence fits within these categories. The core disagreement lies in whether electronic evidence should be treated as physical evidence—due to its tangible and perceptible nature—or as technical evidence, given that it is derived from expert interpretation based on scientific and technological principles.

There are two main doctrinal views:

- The **first view** regards electronic evidence as a modern extension of physical evidence. It can be perceived through the senses, particularly when printed from a computer—its source—similar to other scientific evidence such as weapon traces or DNA.
- The **second view** sees electronic evidence as a distinct type of proof, warranting its own classification as a new category within the evidentiary framework.

2. Doctrinal Classifications of Electronic Evidence

Due to its relatively recent emergence and ongoing evolution, criminal law scholars have not yet fully developed a comprehensive study of electronic evidence. However, some have attempted to classify it into four categories:

1. **Electronic evidence related to computers and their networks**
2. **Electronic evidence related to the Internet.**
3. **Electronic evidence concerning information exchange protocols between global network devices.**
4. **Electronic evidence connected to the World Wide Web.**
5. This classification mirrors doctrinal classifications of computer-related crimes, as explained below:

a. Electronic Evidence Related to Computers and Their Networks:

This includes non-human behaviors that constitute unlawful acts targeting computer devices, whether affecting their hardware, software, or main databases—for example, damaging physical components like printers.

b. Electronic Evidence Related to the World Wide Web:

This includes human conduct involving illegal acts against any document or data on the web, such as information piracy, credit card data theft, or software intellectual property violations. These crimes typically require internet access.

c. Electronic Evidence Related to the Internet:

This refers to illegal actions concerning data transmission mechanisms between users of the global network, such as unauthorized access to restricted sites or the use of false IP addresses to access information unlawfully.

3. Legislative and Judicial Classifications of Electronic Evidence

- Several legislative bodies and judicial authorities have attempted to classify electronic evidence. Among them, the United States has been a pioneer in addressing this issue through legislation and court decisions. The U.S. was the second country, after Sweden, to enact laws criminalizing cybercrime. Notable legislation includes:
- The Fair Credit Reporting Act of 1970,
- The Privacy Act of December 31, 1974,
- The Freedom of Information Act of 1976
- The Electronic Communications Privacy Act of 1986,

among others (Mustafa, 2010, pp. 73–74).

In 2002, the U.S. Department of Justice proposed a classification of electronic evidence into three main categories:

a. Computer-Stored Records:

These are documents that are written and saved electronically. Electronic writing includes all letters, numbers, symbols, or other marks inscribed on electronic, digital, optical, or similar media in a perceptible format (Mansour, 2006, p. 272).

Examples include email—defined as a method of exchanging written messages between devices connected to a network (Ibrahim K., 2008, pp. 101–102)—as well as word processing files and internet chat logs (Farah, p. 59).

b. Computer-Generated Records:

These records are generated automatically by computers without human intervention, such as log files, telephone records, and ATM transaction receipts.

c. Computer-Input and Processed Records:

This type includes records such as financial spreadsheets, where users enter data that is then processed by programs like Excel to produce results. These combine human input with computer processing.

This classification has also been adopted by U.S. courts. Computer records accepted as evidence in court are typically in textual form, either:

- **Stored computer records**, which include documents written by individuals in electronic form (e.g., emails), or

- **Generated computer records**, which originate from system operations (e.g., internet access logs from ISPs).

There is also a **hybrid type**, involving both human input and computer processing—such as whe a defendant enters false income data into a tax program to calculate a lower tax liability.

- However, this classification has been criticized for not covering the full scope of electronic evidence. It primarily addresses text-based records and excludes other forms such as images, audio, graphics, and video. In today's context, communication protocols and software applications play a critical role in committing cybercrimes. For instance, the TCP/IP protocol is one of the most widely used protocols on the internet and can reliably identify both the source device used in a crime and the devices affected by the unlawful act.

Thus, the diversity of electronic evidence indicates that there is no single means of collecting it. It can take various forms but remains classified as electronic evidence—even when converted into another format. Recognizing electronic evidence in legal proceedings often relies on the assumption of its virtual nature, especially in light of the limited technological resources available to criminal courts (Mustafa, 2010, pp. 75–77).

Second Section: Mechanisms for Obtaining Digital Evidence in Proving Cybercrime

In this section, we will examine the **conditions for the admissibility** of digital evidence in criminal matters, the **means of obtaining such evidence**, and its **probative value before criminal courts**.

First: Conditions for the Admissibility of Digital Evidence in Criminal Proceedings

The criminal judge enjoys wide discretionary power in evaluating evidence, including digital evidence. The judge may independently seek the truth by gathering evidence without being bound by predetermined preferences for specific types. Even if the law limits admissible evidence types or requires certain forms of proof, digital evidence remains permissible provided it meets essential legal safeguards.

The legislator has established specific criteria for the admissibility of digital evidence, which serve as safeguards against judicial arbitrariness. These conditions enhance the credibility and proximity of such evidence to the truth, thereby allowing it to be accepted as legitimate proof in criminal cases (Mustafa, 2010, pp. 267–268).

الذي للنص **الإنجليزية اللغة** إلى الترجمة إليك بالطبع،
:الدقيق القانوني المعنى على المحافظة مع به، زودتني

To Accept Digital Evidence in Criminal Trials, Certain Conditions Must Be Met:

For a criminal judge to accept digital evidence and consider it legally binding in terms of probative value, three main conditions must be fulfilled. First, the digital evidence must be obtained lawfully and be admissible. Second, the digital evidence must be subject to discussion and challenge. Third, the judge's conviction must reach a level of certainty. Accordingly, the following are the conditions governing the criminal judge's conviction regarding digital evidence:

1. The Condition of Legality of Digital Evidence:

The criminal judge has the discretion to evaluate digital evidence admissible in a case. For such evidence to be considered admissible, it must be obtained lawfully, with honesty and integrity. The judge must apply the evidence properly and base their conviction on legally accepted digital evidence. The scope of the judge's discretion is limited to admissible evidence (Mustafa, 2010, p. 268). Hence, the legality of digital evidence acts as a major guarantee of individual freedoms. Using unlawful methods to obtain digital evidence results in invalid procedures, rendering such evidence inadmissible for criminal conviction. Unlawful methods include physical or psychological coercion or deception to compel the accused in cybercrimes to reveal access codes or decrypt systems to retrieve electronic evidence (Hamouda, 2003, p. 38).

2. The Condition of Discussing Digital Evidence:

A fundamental principle in criminal proceedings is that the judge must base their verdict on evidence presented and discussed in open court. This requires that the evidence must be documented in the case file and that the parties are granted the opportunity to examine and challenge it. Article 221-2 of the Algerian Code of

Criminal Procedure stipulates:

"The judge may only base their decision on evidence presented and discussed during oral arguments in court."

This applies equally to digital evidence, regardless of its form—whether displayed on a computer screen, stored on disks or magnetic tapes, or printed. All must be subject to courtroom discussion to be used as evidence.

The discussion of digital evidence relies on two fundamental elements

- **First**, the opportunity must be given to both parties to examine and respond to the digital evidence. This respects the right of defense and ensures that the parties can effectively confront the evidence. The principle of confrontation also allows the accused to be informed of the charges, prepare a defense, and have access to legal counsel. It further permits both parties to submit documents, question witnesses and experts, and request any action the judge deems appropriate to uncover the truth.
- **Second**, the digital evidence must be part of the case file to ensure the judge's conviction is based on established facts. For this reason, the legislator requires a written record of the court session to document case events and evidence. This allows the trial judge or any party to refer back to the record for clarification (Mustafa, 2010, pp. 271–273). Algerian law enshrines the principle of confrontation and its legal guarantees in Articles 100 and 101 of the Code of Criminal Procedure.
- As a result, the judge's conviction must stem from their own belief, not the opinion or knowledge of others. Personal knowledge or second-hand opinions cannot form the basis of a conviction. The judge builds their belief through assessment of the strength or weakness of the evidence presented (Rajeh, 2010–2011, p. 413).

3. The Condition That Judicial Conviction Reaches the Level of Certainty:

The judge must reach a **state of certainty** based on digital evidence obtained via electronic means. Certainty is defined as the existence of a truth established through sensory knowledge, free of ambiguity or doubt. This is achieved by the judge inspecting the evidence and drawing logical conclusions to confirm the facts. In criminal judgments, certainty is a general requirement, whether the evidence is traditional or modern like digital evidence.

Digital evidence must be free of doubt. Any uncertainty is interpreted in favor of the accused, based on the principle of the presumption of innocence. If the judge harbors any doubt about the validity of the charge, they must acquit the defendant, in line with the principle of **"in dubio pro reo"** (benefit of the doubt to the accused), as affirmed by Article 45 of the Algerian Constitution.

While judges may reach certainty through sensory or intellectual analysis, determining whether a cybercrime occurred and assigning responsibility requires **scientific knowledge of digital technologies**. Since the criminal judge plays an active role in fact-finding, ignorance in this field could undermine the value of the evidence and result in wrongful acquittals, allowing cybercriminals to escape justice. Therefore, to convict, the judge must achieve a certainty level based on digital evidence, as conviction is a result of certainty.

In Canadian jurisprudence, the prevailing view is that computer-generated outputspossess the required level of certainty for criminal judgments, making them among the best forms of evidence. Similarly, some U.S. laws consider copies of computer-stored data as the best form of evidence, ensuring the principle of certainty is met (Al-Tawalbeh, 2011, p. 8).

Secondly: Methods of Obtaining Digital Evidence in Criminal Matters:

These can be summarized as: **interception of communications, search, expert analysis, and inspection**, as follows:

1. Interception of Communications:

This is among the most crucial modern investigative procedures due to its effectiveness in gathering criminal evidence. It refers to intercepting, recording, or copying communications transmitted through wired or wireless means. Such communications may include data capable of being produced, distributed, stored, received, or displayed.

The Algerian Code of Criminal Procedure regulates this process from **Articles 65 bis 05 to 65 bis 10**. Nota-

bly, **Article 2, clause (w)** of Law No. 09-04 (concerning specific rules for preventing and combating ICT-related crimes) expands the traditional concept of correspondence to include electronic communications, aligning with technological advancements. It defines correspondence as:

"Any transmission, sending, or receiving of signs, signals, writings, images, sounds, or other information by any electronic means."

Hence, correspondence includes any message—physical or digital—transmitted by any means to a specified recipient, excluding books, magazines, newspapers, and periodicals.

Due to its impact on individual privacy and the confidentiality of correspondence—guaranteed by **Article 39** of the 1996 Algerian Constitution—the legislator imposed strict legal conditions to prevent abuse:

- A written authorization from the **public prosecutor** or **investigating judge** is required.
- The authorization must be limited to **4 months**, renewable depending on the investigation.
- It must specify all elements to identify the targeted communications and locations.
- This measure is limited to crimes listed in **Article 65 bis 5**, including offenses against automated data processing systems.

2. Searching and Seizing Digital Criminal Evidence:

Search is one of the most important investigative procedures, often yielding physical evidence that supports the criminal charge. It is generally defined as:

"The act of investigating a person's private domain to find evidence of a committed crime."

However, this conflicts with the **immaterial nature** of digital evidence (Harwal, 2007, p. 223). Searching digital systems refers to collecting data stored or recorded electronically, including data in the system or on storage media.

There are two main types of searches for computer systems:

- **Physical Components Search**: This involves inspecting hardware like the keyboard, mouse, screen, printer, and memory units. This aligns with traditional search concepts as it targets tangible objects and follows legal rules for search.
- **Logical Components Search**: This involves examining software, including operating systems and application programs used to process data. According to **Article 5 of Law No. 04/09**, Algerian law allows judicial authorities and police officers to conduct such searches in cases of ICT-related crimes.

Ertisexpe and Crime Scene Investigation:

A. Expertise:

Judicial expertise is the technical consultation that a judge or investigator resorts to in order to assist in forming a conviction regarding matters that require specialized scientific knowledge or expertise. Thus, expertise is a means to interpret evidence technically using scientific knowledge. In essence, it is not considered independent evidence but rather a technical evaluation of such evidence.

To carry out this expertise, a technically specialized individual in a certain scientific or technical field is required—one who, through knowledge and experience, can provide an opinion on a matter requiring special technical assessment. This individual is known as an expert. While the use of technical experts in traditional crimes is necessary, their involvement in cybercrime is even more essential due to the high level of skill and computer knowledge required to extract digital forensic evidence. Therefore, it is imperative to seek the help of a qualified and specialized technical expert.

Due to the nature of the expert's work in this field, Algerian legislators have organized the process of expertise and its procedures through Articles 143 to 156 of the Algerian Code of Criminal Procedure, with Article 143 explicitly addressing this.

B. Crime Scene Investigation:

For digital crime scene investigations to have practical value in uncovering the circumstances of the crime, several technical steps and procedures must be followed. Some of these steps are preparatory, including task delegation among technicians and gathering preliminary information about the crime scene and the number and types of devices to be examined, in order to determine the technical handling capabilities.

Other steps occur during and after the investigation. Technicians document and photograph the computer and all its physical components, especially the rear parts, while recording the date, time, and place of each photograph. In addition, they observe and record the status of connections and cables linked to peripherals, preserve any discarded or torn documents from the trash, and inspect tapes and CDs.

Afterward, the computer is powered on to search for digital traces left by the user. This is done using various technical tools to access logs and files. During this phase, all wired and wireless internet connections must be disabled to avoid tampering or intentional remote destruction of digital evidence. When digital data or information is found, digital forensic evidence preservation rules must be followed to ensure careful storage and later examination and use.

Third: The Evidentiary Value of Digital Evidence:

The application of the principle of judicial conviction by the criminal judge regarding digital evidence is reflected in both practice and jurisprudence. Digital evidence is not treated as a standalone proof but is subject to general evidentiary principles like any other form of evidence. Hence, digital evidence is not an exception—it is assessed under the same general rules followed by judicial decisions (Madrel, 2019, p. 72).

The Algerian legislator has enshrined the principle of personal conviction for the criminal judge in Article 307 of the Algerian Code of Criminal Procedure, which states:

"Before the court exits the courtroom, the president shall read the following instructions, which are also displayed in large letters in the deliberation room:

'The law does not require judges to justify the means through which they formed their conviction, nor does it prescribe specific rules for assessing the sufficiency of any evidence. Rather, it instructs them to silently and thoughtfully question their consciences, considering the impact the evidence and defense had on their understanding. The law imposes only this one question that encompasses the full scope of their duty: Do you have personal conviction?'"

Similarly, Article 212 confirms that crimes can be proven by any means of criminal evidence and that the judge may base their ruling on personal conviction. The Supreme Court emphasizes this principle before the Criminal Court and has reaffirmed it through numerous rulings.

The judge's conviction must be based on legally sound evidence. If not, the judge may dismiss the evidence. The criminal judge has wide discretion in weighing evidence and choosing from any persuasive indication as proof for their ruling. The judge's role is to uncover the truth using strong and unequivocal evidence. Criminal justice is based on the judge's freedom to assess and compare the available evidence. If the judge is not convinced or confident in some evidence, they may disregard it during the evaluation.

The criminal judge has complete freedom to exclude any ineffective evidence and is not obliged to list all the evidence considered in court. The judge only needs to cite the evidence sufficient to support their conviction, in a logical and rational manner.

Conclusion:

The topic of digital evidence as a tool for criminal proof is among the most important subjects due to the ongoing development of electronic evidence and the tools for extracting it from computer systems.

Regardless of its scientific or technical merit, evidence only fulfills its role through the presence of a criminal judge who possesses wide discretion to detect errors, manipulation, or fraud in digital evidence and to transform scientific truth into judicial truth.

The truth always requires proof, and as such, the methods for extracting evidence must evolve. Accordingly, the digital forensic evidence derived from computers, the internet, or any other data-processing device is essentially magnetic or electrical pulses that can be compiled and analyzed using specialized software to produce usable information or data during investigation and trial.

As a result, digital evidence has asserted itself as a valid and powerful proof in criminal law, despite its unique

and complex nature and the procedural challenges it poses.

Recommendations and Suggestions:

Based on this study, we offer the following recommendations:

- Expand the definition of cybercrimes in the Algerian Penal Code to cover all possible offenses.
- Establish a comprehensive database of cybercrimes, including their methods, types, and characteristics, for future reference.
- Organize awareness campaigns and educational seminars on internet risks and cybercrimes to foster a culture of information security and user protection.
- Train judicial staff to understand the nature of electronic evidence and enhance the training of experts, investigators, and judges in handling cybercrimes.
- Amend criminal procedure rules governing digital evidence collection to align with its unique nature.
- Improve cooperation between the justice system and telecom providers to facilitate access to digital evidence in support of investigations.
- Strengthen international cooperation and leverage foreign expertise in training specialized experts and enhancing the use of digital forensic evidence.
- Continuously upgrade analytical tools for data storage and disk imaging.
- Regularly raise public awareness about cybercrime risks and criminal techniques through media channels.
- Include information systems and cybercrime subjects in law, police, and judicial training programs. Require applicants to hold university degrees in computer science or networking

References

1. Ibrahim, H. M. *Electronic Litigation*. Egypt: Dar Al-Fikr Al-Jami'i, 2008.
2. Ibrahim, M. *The Art of Criminal Investigation in Cybercrimes*. Egypt: Dar Al-Fikr Al-Jami'i.
3. Abu Al-Qasim, A. *Physical Criminal Evidence and Its Role in Proving Hudud and Qisas Crimes*. Saudi Arabia: Publishing House at the Arab Center for Studies and Training, 1993.
4. Al-Bushra, M. A. *Digital Forensic Evidence (Its Concept and Role in Proof)*. Saudi Arabia: Naif Arab University for Security Sciences, 1995.
5. Al-Husseini, A. A. *Criminal Investigation and Modern Means of Crime Detection*. Lebanon: Al-Halabi Legal Publications, 2015.
6. Al-Halabi, K. A. *Investigation Procedures in Computer and Internet Crimes*. Jordan: Dar Al-Thaqafa for Publishing and Distribution, 2011.
7. Al-Mutlab, M. A. *Digital Criminal Investigation in Computer and Internet Crimes*. Egypt: Dar Al-Kutub Al-Qanuniya, 2006.
8. Thunayan, T. N. *Proving Cybercrime – A Foundational and Applied Study*. Saudi Arabia: Naif Arab University for Security Sciences, 2012.
9. Rajeh, F. M. *Information Crimes in Algerian and Yemeni Law*. Algeria: Faculty of Law – University of Algiers, 2010–2011.
10. Abdul-Mutalib, T. *Criminal Evidence Using Digital Evidence*. M'sila: Faculty of Law and Political Science, University of M'sila, 2014–2015.
11. Onwuadiamu G. (2025), Cybercrime in criminology; A systematic review of criminological theories, methods, and concepts, Journal of Economic Criminology, Volume 8, 2025,100136, ISSN 2949-7914, https://doi.org/10.1016/j.jeconc.2025.100136.https://www.sciencedirect.com/science/article/pii/S2949791425000120
12. Ezzat, F. M. *Electronic Evidence in Criminal, Civil, and Commercial Matters*. Egypt: Dar Al-Fikr wa Al-Qanun, 2010.
13. Farah, M. *Modern Means of Evidence in Law*. Algeria: Dar Al-Huda for Printing, Publishing, and Distribution.
14. Farghali, A. A., and Mohammed Obaid Saif, S. A. *Criminal Evidence Through Digital Evidence from Legal and Technical Aspects (A Comparative Applied Study)*. Saudi Arabia: Naif Arab University for Security Sciences, 2007.
15. Madreel, K. *Digital Evidence in Criminal Matters*. Bouira: Master's Thesis, Faculty of Law and Political Science, Akli Mohand Oulhadj University, 2019.

16. Mostafa, A. B. *The Legal Weight of Electronic Evidence in Criminal Proof in Algerian and Comparative Law*. Alexandria: Dar Al-Jami'a, 2010.
17. Mansour, M. H. *Traditional and Electronic Evidence*. Egypt: Dar Al-Fikr Al-Jami'i, 2006.
18. Harwal, N. H. *Procedural Aspects of Internet Crimes During the Evidence-Gathering Stage (A Comparative Study)*. Egypt: Dar Al-Fikr Al-Jami'i, 2007.
19. Younes, A. M. *Digital Evidence (Digitale Evidence)*. Egypt, 2006