Volume: 9 Issue: 3 Month: 9, Year: 2026
P.P 52 - 62
مجلة البحوث القانونية والاقتصادية
JOURNAL OF LEGAL AND ECONOMIC RESEARCH

DIGITAL EVIDENCE AND THE DIFFICULTIES OF ITS LEGAL ESTABLISHMENT

Arbia FEGHOUL*
University of Blida, Lounisi Ali- Algeria
a.feghoul@univ-blida2.dz
Laboratory of Digitalization and Law in Algeria

Send Article Date: 02-07-2026	Date of acceptance of the article: 20-08-2026

Abstract:

Since we have entered an era in which the means of committing crime have evolved from traditional to electronic, criminals have begun exploiting scientific progress and technological development to commit crimes through methods that enable them to hide their traces, making it difficult to detect them and identify the perpetrator using traditional means of proof.

Electronic evidence has, in turn, become one of the newest scientific and technical means, as well as the most advanced and widely used, for proving electronic crimes. Its use requires compliance with the limits established by special laws and the rules of the Code of Criminal Procedure, with the aim of achieving procedural legality.

Keywords: Electronic Evidence; Criminal Proof; Electronic Crime; Technological Development.

Introduction:

The electronic field has facilitated many aspects of individuals' lives in different fields, and due to the important role it plays in daily life, it has become impossible to dispense with its use at the present time. However, on the other hand, a special type of crime has emerged, known as electronic crime, which represents a serious and newly emerging criminal phenomenon whose scene is virtual, while its consequences affect the real world, threatening the security and stability of states, as well as individuals' right to privacy. Likewise, the diversity of the methods used to commit this crime has led to risks and losses that threaten the national security and sovereignty of states, as

* Arbia FEGHOUL.

well as the loss of confidence in technology and fears of undermining the creativity of the human mind.

Therefore, it has become necessary to confront these newly emerging crimes by discovering evidence to prove them, through which guilt or innocence can be established, especially since this evidence differs completely from the criminal evidence used in traditional crimes. Because these newly emerging crimes are of a special nature, their particularity is clearly reflected in the manner and methods of their commission, the multiplicity of their perpetrators, and the ease with which their evidence can be tampered with. As a result, it has become difficult to discover and prove them at the same time. Therefore, we raise the following problem:

What is electronic evidence, what is its role in proving electronic crime, and what are the difficulties related to it?

The answer to this problem is presented through two sections:

- The first section: The concept of electronic evidence. (Definitions of electronic evidence, characteristics of electronic evidence, and types of electronic evidence.)
- The second section: The role of electronic evidence in proving electronic crime and the difficulties related to it. (The meaning of proof, the conditions for the strength of evidence in criminal proof, and the difficulties of proving electronic evidence.)

1- The Concept of Electronic Evidence

The occurrence of electronic crime and its attribution to its perpetrator require electronic evidence on which the judge relies to ascertain the truth of the facts presented before the court. Therefore, it is necessary to define this evidence and clarify the characteristics that distinguish it, as well as the types that are considered admissible means of proof before the criminal judiciary. This is what we will address in the following points:

1.1- Definition of Electronic Evidence:

The definitions that have been given regarding electronic evidence are numerous. Some researchers have provided broad definitions of this evidence, while others have provided narrow definitions, which we will address as follows:

1.1.1- Broad Definitions of Electronic Evidence:

- Electronic evidence is defined as: "Information that is accepted by logic and reason and relied upon by science, which is obtained through legal and scientific procedures by translating computational data stored in computer devices or communication networks. It can be used at any stage of the investigation or trial to prove the truth of an act or thing related to a crime, an offender, or a victim." (Sarah, 2022-2023, p. 207).
- Electronic evidence is also defined as: "Evidence derived from software information systems, computer devices, equipment and tools, or communication networks through legal and technical procedures for submission to the judiciary after being scientifically analyzed or interpreted in the form of written texts, drawings, images, forms, and sounds to prove the occurrence of the crime and to determine acquittal or conviction." (Taheri, 2023, p. 255).

1.1.2- Narrow Definitions of Electronic Evidence:

- Electronic evidence is defined as: "Data that can be prepared or stored in digital form in such a way that enables the computer to accomplish something." (Imane & Yahya, 2025, p. 544).
- The International Organization on Computer Evidence (IOCE) also defined it as: "Information with potential value that is stored or transmitted in digital form." (Al-Otaibi, 2020, p. 11).

Through these definitions selected from among many others, it becomes clear that electronic evidence can be presented to the judiciary as criminal evidence suitable for proving a crime.

1.2- Characteristics of Electronic Evidence:

The special nature of the electronic environment, which includes multiple types of electronic data that can be used as electronic criminal evidence, as well as the special nature of this type of evidence, distinguishes it from other types of evidence through the following characteristics:

- Evidence that differs from physical evidence: It is intangible evidence that cannot be perceived by the naked senses. Rather, it requires technological means such as computers and

smartphones to display and understand it (Mohammed & Mohammed, 2025, p. 64).

- Evidence capable of copying and multiplicity: Electronic evidence can be copied an unlimited number of times without the copies losing their value or conformity with the original. This makes it difficult to destroy completely and enhances its permanence compared to paper documents, which are affected by factors such as humidity and dust (Msikah, 2022, p. 142).
- Evidence with a fragile nature: Despite its permanence, it can be modified, altered, or even deleted easily without leaving a clear trace for non-specialists. This raises fundamental challenges regarding its reliability and makes examining its integrity a decisive matter (Taheri, 2023, p. 294).
- Evidence with a cross-border nature: Electronic evidence can move through communication networks in fractions of a second, crossing the geographical borders of states. This raises challenges related to judicial jurisdiction and the applicable law (Mohammed & Mohammed, 2025, p. 64).
- Technical and evolving evidence: Due to its complex technical nature, electronic evidence often requires specialized technical expertise to analyze it, verify its integrity, and present it to the judiciary in a comprehensible and useful manner. Also, electronic evidence, in its essence, depends on advanced means that change and evolve continuously with technological progress, making it evidence whose forms are continuously renewed by their very nature (Mohammed & Mohammed, 2025, p. 63).

1.3- Types of Electronic Evidence:

The rapid spread of electronic means of communication has led to an increase in the circulation of electronic information and data in the virtual environment, which can be downloaded, stored, or documented by various means, such as magnetic disks, digital video discs, or other electronic media. Therefore, digital evidence has multiple types. However, what concerns us are the digital pieces of evidence that are prepared to serve as a means of proof, and they are of two types (Sarah, 2022-2023, p. 215):

- The first type: This type is created automatically by the machine. These records are considered outputs of the machine in which humans did not contribute to their creation, such as telephone records and automated teller machine receipts.
- The second type: This type consists of records in which one part is stored through human input, while another part is subsequently created by the machine. Examples include data entered into a computer and processed through special programs, such as performing arithmetic operations on those data.

2- The role of electronic evidence in proving electronic crime and the difficulties related to it

Electronic evidence has great importance in protecting rights and transactions and establishing them for their rightful owners, especially since most transactions are now carried out electronically. However, there are multiple difficulties in its application, which we will discuss later after clarifying the meaning of proof, a term that legislation has not defined but has instead left to legal scholarship.

2.1- The Meaning of Proof:

Proof has great importance in the field of crime, which has prompted legal scholars to research and examine it. Therefore, we will address its linguistic, terminological, and legal meanings.

2.1.1- Its Linguistic Meaning:

Proof is defined in *Lisan al-Arab* as: "It became established, firmly established, and fixed, so it is established." Proof is the evidence, the proof, the testimony, or the argument. It is also called *thabt* because of what it leads to in establishing the right for its owner. Thus, it is said: "I do not judge such-and-such except by proving the thing through it." Also, restricting a right by evidence is called proof, and the word *thabt*is used figuratively for one who is an authority, that is, trustworthy in his narration (Bahnas, 2018, p. 17).

2.1.2- Its Terminological Meaning:

By referring to the books of classical jurisprudence, we find that no definition of proof in the terminological sense was provided. Rather, they intended by it its linguistic meaning, which is establishing the argument regarding one of the facts, whether before the judge or before someone else.

The specific meaning of proof is establishing evidence before the judiciary through the methods specified by the Sharia regarding a right or a specific fact upon which legal effects have resulted. It is, therefore, the establishment of an argument by clear evidence in the event of a dispute before the judiciary (Ahmed & Ibrahim, 2021, p. 107).

2.1.3- Its Legal Meaning:

Proof in the legal sense is the establishment of evidence before the judiciary regarding the existence of a legal fact, by the manner or methods specified by law and subject to the restrictions it has laid down concerning the existence of a disputed legal fact (Bouhalit, 2019, p. 396).

2.2- Conditions for the Strength of Electronic Evidence in Criminal Proof:

Reaching unlawful acts committed by electronic means that occur through forgery, modification, or deletion of processed data, whether during its input, storage, or output, requires scientific and technical evidence capable of proving their occurrence and attributing them to the persons accused of committing them.

This is the function of electronic evidence, which requires compliance with certain conditions in order to establish its evidentiary strength. These conditions are represented in the following four important points:

- Legitimacy of Seizing Electronic Evidence The procedures adopted to obtain electronic evidence must be lawful, not prohibited by law, and subject to the supervision of the court. Since these procedures are intended to preserve the electronic evidence and maintain it in the condition in which it was seized, the evidence must be clear and free from ambiguity. Any evidence obtained by unlawful methods is invalid, and the judge has discretionary authority to accept or exclude it (Taheri, 2023, p. 296).
- Certainty of Electronic Evidence: The trial judge must verify the reliability of the electronic evidence before relying on it because the nature of electronic evidence requires the judge to seek the assistance of a specialized expert who can understand it and determine its implications, with the aim of enabling the

judge to understand the nature of the contents of the electronic evidence (Ibrahim, 2023, p. 61).

- The Necessity of Discussing Electronic Evidence: For the judge to be convinced by the electronic evidence, it is required that it be discussed in the presence of all parties to the dispute in accordance with the principles of confrontation, transparency, and the public nature of the trial, so that the judge ultimately reaches a conviction and issues a judgment that satisfies his conscience (Bouhalit, 2019, p. 411).

2.3- The Difficulty of Proving Electronic Evidence:

Electronic evidence raises multiple difficulties in proving it due to its special nature. Before being convinced by it, the criminal judge may be required to determine its scientific value by seeking the assistance of experts and specialists, then examine the circumstances and conditions in which the evidence was found, which may negatively affect the judge's conviction, leading him to reject it if he finds that its existence does not logically correspond with the facts of the case. Among these difficulties, we mention:

2.3.1- Difficulties Related to the Electronic Evidence Itself:

- Electronic evidence proving cybercrimes is non-material and invisible. It consists of electronically recorded data with very high density and depends on optical or magnetic storage media. It does not reveal a specific identity. Usually, any modification or tampering does not leave any trace.
- Electronic evidence can be easily erased by the offender. The offender may destroy the evidence of conviction within a short period. In addition, this act can easily be made to appear as though it resulted from an error in the computer system or the network.
- There is difficulty in accessing the evidence, as the perpetrators of cybercrimes protect their devices and websites with passwords, codes, or ciphers in order to hinder access to the data recorded on them.
- There is a huge volume of information and data that must be examined. In other words, there is an enormous amount of data found on electronic devices and the internet websites visited by the offender, which constitutes an obstacle for the investigating

authorities, as they cannot ascertain the validity of the accusation attributed to the offender except by examining that data. This requires a long period of time and a high level of technical expertise (Ahmed A. M., 2020, p. 101).

2.3.2- Difficulties Related to the Nature of Cybercrime:

- Cybercrime is invisible in most of its forms, as the victim does not notice it and may not even realize that it has occurred. It also leaves no material traces through which its perpetrator can be identified because it takes place in the virtual world, and its scene is the computer and the information network. The cybercriminal leaves behind no material traces such as the weapon used in the crime or fingerprints and does not need to break locks or move stolen property to commit the crime. Rather, it is sufficient to have a computer connected to the Internet (Ahmed A. M., 2020, p. 102).
- Likewise, cybercrime is committed in multiple places and crosses geographical borders. The cybercriminal may be in one country, the crime may be committed in a second country, and the resulting effects may occur in a third country. The multiplicity of the locations of the crime and their remoteness increase the difficulty of discovering it and, consequently, proving it (Al-Maraghi, 2017, p. 62).

2.3.3- Difficulties Related to the Human Factor:

Difficulties related to the victims: These are represented by their reluctance to report crimes, which is considered one of the greatest difficulties facing the process of search and investigation, whether the victims are individuals or institutions.

As for individuals, they refrain from submitting a report out of fear of the society surrounding them, fear of scandal, and fear of being deprived of certain services related to public order (Al-Maraghi, 2017, p. 119).

As for institutions, they refrain from submitting a report to avoid the resulting damage, as it may lead to a loss of confidence in their reputation and competence. In addition, inspection operations carried out by the investigating authorities may expose the institutions' secrets or allow access to their data and information, which they seek to keep confidential (Ben Sghir, 2014, p. 75).

Difficulties related to the investigation and inquiry authorities: These may be represented by the lack of experience among police officers, investigators, and judges. They may not have sufficient knowledge of computers, the Internet, electronic evidence, and how to deal with it. This difficulty is considered a major obstacle to the process of collecting electronic evidence. This is because the novelty of electronic crimes and their advanced technologies require judicial police officers and the authorities responsible for investigation and adjudication to be trained and familiar with technical expertise in the field of digital crimes, enabling them to detect such crimes and prosecute their perpetrators judicially (Hijazi, 2009, p. 108).

2.4- Difficulties Related to the Judicial Aspect:

Lack of international cooperation in combating electronic crimes: We have previously studied that digital crimes cross geographical borders and can be committed remotely, which increases the difficulty of detecting and proving them. Therefore, international cooperation is necessary to confront them. However, several obstacles stand in the way of achieving this, the most important of which are (Al-Maraghi, 2017, p. 126):

- The difficulty of unifying the concepts related to electronic crime among different countries.
- Differences in the procedural systems related to inquiry and investigation of these crimes among different countries.
- The absence of cooperation among different countries in confronting electronic crimes, verifying them, and prosecuting their perpetrators.
- The problem of judicial jurisdiction: A crime that occurs within the territory of a particular state is subject to its criminal law in accordance with the well-established principle of territoriality. However, the Internet is a global network that is not limited by geographical borders and is therefore beyond the supervision or control of any single authority. Consequently, its perpetrator cannot easily be subjected to the authority of a specific criminal law (Abdelhafid, 2022, p. 305).

Conclusion:

No one can deny the great importance of electronic evidence in criminal proceedings. Establishing the occurrence of an electronic

crime and attributing it to its perpetrator is a matter of utmost importance, especially since electronic crime has characteristics that differ from those of traditional crime. The search for electronic evidence also depends on precise scientific standards used by experts and specialists while observing the limits set by law. If these limits are not observed, the procedure becomes void, as does the evidence derived from it. The reason for this is that there are many difficulties in proving electronic crime.

Based on the above, the following findings and recommendations can be presented:

Results:

- The principle of legality is one of the most important restrictions regulating the authority of the criminal judge in dealing with electronic evidence and accepting it. While assessing the evidence, the judge is obliged to observe the requirement of legality.
- Electronic evidence proving electronic crimes is non-material and invisible.
- The criminal judge bases the judgment only on valid evidence resulting from lawful procedures.

Practical suggestions:

- The necessity of raising society's awareness and promoting a new social culture regarding unlawful acts related to the electronic environment, for which the responsible person is subject to criminal penalties after evidence has been obtained to prove them.
- Enacting modern and comprehensive laws to confront and combat electronic crime while preserving the principle of criminal legality.
- Conducting training courses on how to detect electronic crimes, especially for police officers, investigators, and judges.
- Cooperation among the international community to combat electronic crime while respecting the national sovereignty of the states concerned.

References:

Abdelhafid, M. (2022). Al-Zajr al-Jinai lil-Jarimah al-Elektroniyyah: Al-Tahaddiyat wa al-Afaq. *Qanouni Journal, 3*(13).

Ahmed, A. M. (2020). Al-Adillah al-Raqmiyyah wa Hujjatuha fi Ithbat al-Jaraim al-Elektroniyyah: Dirasah Fiqhiyyah Muqaranah. *Scientific Journal of the Faculty of Sharia and Law, Assiut*(32 (Issue 2)), Part 2.

Ahmed, B. M., & Ibrahim, E. (2021). Dawr al-Adillah al-Raqmiyyah fi al-Ithbat al-Jinai. *Journal of Human Sciences, 5*(1).

Al-Maraghi, A. A. (2017). *Al-Jarimah al-Elektroniyyah wa Dawr al-Qanun al-Jinai fi al-Hadd Minha: Dirasah Tahliliyyah Tasiliyyah Muqaranah* (1st ed.). Cairo: National Center for Legal Publications.

Al-Otaibi, Z. b. (2020). Dirasah Istitlaiyyah Hawla Hujjiyyat al-Adillah al-Raqmiyyah fi Ithbat al-Jaraim al-Malumatiyyah. *Comprehensive Multidisciplinary Electronic Journal*(29).

Bahnas, Y. H. (2018). *Al-Ithbat bil-Wasail al-Ilmiyyah al-Hadithah wa Sultat al-Qadi al-Jinai fi Taqdiriha.* Arab Studies Center for Publishing and Distribution.

Ben Sghir, A. a.-M. (2014). Al-Tabiah al-Khassah lil-Jarimah al-Murtakabah Abr al-Internet fi al-Tashri al-Jazairi wa al-Tashri al-Muqaran. *Journal of Rights and Freedoms*(2).

Bouhalit, Y. (2019). *Al-Jaraim al-Elektroniyyah wa al-Wiqayah Minha fi al-Qanun al-Jazairi.* Alexandria: Dar al-Jami'ah al-Jadidah.

Hijazi, A. a.-F. (2009). *Nahwa Siyaghat Nazariyyah Ammah fi Ilm al-Jarimah wa al-Mujrim al-Malumati* (1st ed.). Alexandria: Munshaat al-Maarif.

Ibrahim, K. M. (2023). *Al-Khibrah al-Qadaiyyah fi al-Jaraim al-Malumatiyyah.* Alexandria: Dar al-Fikr al-Jami.

Imane, B., & Yahya, D. (2025). Athar Khususiyyat Ijraat al-Tahqiq fi al-Jaraim al-Malumatiyyah ala Hujjiyyat al-Dalil al-Raqmi fi al-Ithbat. *Journal of Rights and Freedoms, 13*(2).

Mohammed, H. A., & Mohammed, S. H. (2025). Al-Dalil al-Raqmi fi Nizam al-Ithbat al-Saudi: Hujjiyyah wa Muwajahah lil-Tahaddiyat al-Mustajiddah. *Al-Muhami Journal, 21*(2).

Msikah, M. A.-S. (2022). Mafhum al-Jaraim al-Mustahdathah wa Tabiatuha al-Qanuniyyah. *Journal of Legal and Political Studies, 8*(10).

Sarah, M. (2022-2023). Mashruiyyat al-Dalil al-Jinai. *Doctoral Dissertation in Criminal Law and Criminology*. Algiers, Algeria: University of Algiers 1, Faculty of Law.

Taheri, H. (2023). *Ijraat Jam al-Adillah wa al-Tahqiqat al-Awwaliyyah fi al-Jaraim al-Malumatiyyah: Al-Muhakamah al-Elektroniyyah.* Oum El Bouaghi: Dar al-Ula for Printing, Publishing, Translation, and Distribution.