Pegem Journal of Education and Instruction, Vol. 16, No. 1, 2026 (pp. 1198-1220)

RESEARCH ARTICLE WWW.PEGEGOG.NET

Mechanisms for Adapting Criminal Investigations to the Information Technology Environment

Dr. Samia Alilaouar

Faculty of Law and Political Science, University of August 20, 1955 – Skikda, Algeria
Email: s.alilaouar@univ-skikda.dz

Received:12.02.2025 ; Accepted:15.06.2025 ; Published:22.01.2026

Abstract:

Crimes have always been closely associated with the emergence of early human societies. Initially simple, reflecting the simplicity of those primitive societies, they have continually evolved and become increasingly complex in line with the rapid transformations experienced by humanity. With the advent of the technological and digital era, new forms of crime have emerged, notably cybercrime, which requires specific mechanisms for detection and investigation, foremost among them digital investigation.

Keywords: Crime evolution, Cybercrimes, Digital crime, Digital investigation.

Introduction:

Crimes constitute an eternal phenomenon that emerged with the appearance of the earliest societies; indeed, they predate them by a long margin. As these societies evolved and their populations increased, crimes assumed greater complexity in form and degree, which necessitated the search for methods and mechanisms to confront them. The task of investigating crimes and uncovering their circumstances was entrusted to individuals known as investigators.

Criminal investigations have passed through several stages before reaching their current form, beginning with the system of informants and inspections employed to guard the property and tombs of the ancient Egyptians, and moving through what was known among ancient Arabs as al-bash ‘a, which involved heating a piece of iron and requiring the accused to lick it. If the accused feared doing so, he was deemed the perpetrator, based on the assumption that he would be tense and that his bodily functions— “including saliva secretion”—would be unstable, preventing proper moistening of the mouth and causing him to fear licking the iron because it would burn him. By contrast, the innocent person would be relaxed, with a moist mouth, and thus would not recoil; even if he licked the heated iron, he would not be greatly

affected.[1] Torture, which prevailed in European states during the Middle Ages as a system for uncovering crimes, was likewise based on the principle that "confession is the master of evidence," whereby confessions were sometimes forcibly and unjustly extracted. This development ultimately gave way to reliance on audio and visual media and communication technologies, as well as on fingerprint science, which accompanied the tremendous technological advancement.

In our current era, the subject of criminal investigations continues to evolve, particularly in light of the emergence of a new type of crime that is committed from remote locations and does not recognize the territorial boundaries of states, including cybercrimes or information crimes, as some term them.

Accordingly, it may be said that information crimes are newly emerging crimes that appeared with the advent of digital devices. Although they were not as widespread in the past as they are today, rapid technological developments, in addition to certain global circumstances, have contributed to their proliferation, especially over the past few years. This has rendered traditional criminal investigation mechanisms incapable of pursuing and proving them, thereby creating the need to adapt these mechanisms to the information technology environment by seeking to develop investigative and inquiry tools and to update legal texts in a manner that fulfils this purpose. Hence, and on the occasion of this study, we approach the research problem through the following question:

To what extent are traditional criminal investigation mechanisms effective, and how have they been affected by the rapid development in the field of information technology? To what extent are they capable of confronting information crimes?

In this context, and through this research paper, we shall present—within a dual-framework plan—the legal and technical foundations for adapting criminal investigations to the information technology environment (First), and we shall address digital investigation as a mechanism for uncovering cybercrimes (Second).

First: The Legal and Technical Foundations for Adapting Criminal Investigations to the Information Technology Environment:

The development of societies has contributed to the emergence of more serious crimes that do not only affect the society in which they occur, but whose impact extends to other societies and states as well. These crimes are characterized by a high degree of shrewdness, cunning, and planning aimed at concealing them, including cybercrimes (digital crimes). In order to keep pace with such crimes and uncover them, it has become necessary for the authorities entrusted with criminal investigation tasks to devise methods that correspond to their development, rather than relying on traditional investigative techniques that have

[1] Naji, Yaacoub; Othmani, Abdel Rahman. Criminal Investigation and Inquiry through Traditional Methods. Journal of Legal Studies, vol. 7, no. 2, 2020, p. 529.

become almost incapable of confronting them.

1 – The Legal Particularity of Information Crime and Its Impact on Criminal Investigation:

As previously indicated, information crimes are new offenses that accompany the major technological developments affecting all aspects of life, which have transformed the world into a small village under what is known as globalization. Before examining this emerging type of crime and clarifying its particularity and the means of uncovering its circumstances, it is necessary to take a brief look at criminal investigation and its traditional mechanisms.

A – The Concept of Criminal Investigation:

The need for criminal investigations arises whenever an incident or crime occurs and its manner and circumstances are obscure or unknown. It is carried out by persons legally authorized to do so. Investigation, in general, means the search for the causes and motives behind the occurrence of various phenomena and events. It may be said that the search for motives and causes of incidents and the like stems from human nature, which requires finding answers for everything that happens or surrounds human beings.

A-1 – Definition of Criminal Investigation and Its Objectives:

Criminal investigation refers to the adoption of methods and techniques leading to the uncovering of facts related to a committed crime or one about to be committed, with the aim of reaching its perpetrators or planners, apprehending them, and bringing them to trial. Criminal investigation is carried out by the criminal investigator, a person entrusted by law with the task of uncovering the circumstances of crimes, searching for their perpetrators and all that surrounds them, and bringing offenders to justice. [1]

¬ **Definition of Criminal Investigation:**

Criminal investigation has been defined as: "A set of procedures undertaken by investigation authorities as specifically prescribed by law, with the aim of scrutinizing evidence and uncovering the truth prior to the trial stage."[2]

It has also been defined as: "A set of legal procedures directly carried out by police agencies and supported by criminal law, and which are prior to the commission of the crime or concurrent with it." [3]

Criminal investigation has likewise been defined as: "A set of procedures aimed at searching for and uncovering evidence concerning the committed crime, and then determining the sufficiency of such evidence to refer the offender to trial, exercised by a person (primarily investigators and judicial police officers, and secondarily investigating judges) entrusted with the authority to take the necessary

[1] Arabi, Ahmed. Criminal Investigation. 1st ed., Dubai Police Academy, United Arab Emirates, 2021, p. 16

[2] Salama, Mamoun Mohamed. Criminal Procedure in Egyptian Legislation. Vol. 1, Dar Al-Nahda Al-Arabiya, Cairo, 2008, p. 641

[3] Naji, Yaacoub; Othmani, Abdel Rahman. Criminal Investigation and Inquiry through Traditional Methods, previously cited, p. 527.

measures, using lawful and legal means with respect to crimes that come to his knowledge, with the aim of uncovering their circumstances and bringing their perpetrators to trial."[1]

In light of the above, we can define criminal investigation as: the first and most important stage of criminal proceedings. It consists of a set of legal procedures to which investigators or investigating judges' resort, each according to their mandate, in an attempt to unravel the mystery of crimes and their perpetrators, and to inquire into the causes, place, and time of their occurrence to reach the perpetrators before bringing them to trial. It can also precede crimes and aim to prevent their occurrence, in case information is received that a crime is about to be committed.

- **The Objective of Criminal Investigations:** From the previous definitions, we can deduce some objectives of criminal investigation, the most important of which are:

Confirming the occurrence of a specific crime: One of the most important objectives of criminal investigation is to prove the occurrence of the crime. It is inconceivable to accuse someone without confirming their involvement in what they are accused of, which is achieved by following effective and legal investigation methods. Furthermore, no one may be brought to trial and subjected to the appropriate penalty for their act before confirming their guilt in what is attributed to them.

Determining the place and time of the crime: Criminal investigation also aims to determine the time and place of crimes, as these two procedures are important in proving or disproving the perpetrator's involvement. Determining them shows whether the person is related to the crime or not through their presence or absence from the crime scene at the time of its commission, thus using them as evidence for conviction or acquittal.

Knowing how it was committed: Investigators, when conducting a criminal investigation, seek to determine how the crime was committed, which is a factor that helps uncover its circumstances. It aims to know the causes and motives leading to its commission and determines the approach to be followed in the investigation.

Apprehending and bringing offenders to trial: We can consider apprehending the perpetrators and bringing them to trial the supreme goal of investigation and the primary reason for conducting it in the first place. It is inconceivable to conduct an investigation without seeking to arrest the offenders and subject them to penalties commensurate with their actions.

A-2 – Mechanisms of Criminal Investigation:

- **Inspection:**

Inspection is considered one of the most important means of criminal investigation, and its purpose is to verify the material facts and everything related to the crime. In this process, the criminal

[1] Abdelkader, Falah; Ait Abdelmalek, Nadia. Criminal Investigation in Cybercrimes and Their Proof. Al-Ustadh Al-Baheth Journal for Legal and Political Studies, vol. 4, no. 2, 2019, p. 1695.

investigator proceeds to the scene of the incident and observes the crime scene and everything that may assist in reaching the perpetrator, such as monitoring and examining all persons present at or who were at the crime scene, as well as observing objects and traces found there, such as tables, chairs, and others, and how they are positioned, while avoiding touching them so as not to affect the results of the investigation. Through inspection, the investigator aims to discover a set of facts, including confirming the occurrence of the criminal act, identifying the perpetrator, determining the type of crime, and its motives

For inspection and the subsequent procedures to be valid—given that it constitutes the cornerstone of criminal investigation and its first measure—it must be accompanied by a set of conditions, the most important of which are:

• Speed in proceeding to the crime scene in order to collect the greatest possible amount of evidence and traces that may be erased if arrival is delayed.

• Securing the crime scene so that it is not tampered with and so that evidence and traces that may contribute to uncovering the circumstances of the crime and reaching the perpetrator are not lost.

• Prioritizing and working in an organized manner so that no detail that may help solve the mystery of the crime is overlooked.

• Strength of observation and deliberation in analysing the facts.

• **Examination and Recourse to Experts:**

This is done by carefully scrutinizing everything left behind by the offender after committing the act, whether visible or concealed. The offender may leave items related to his person, such as hair or bloodstains, or a tool used to commit the crime, such as a stick or a knife, for example. Experts may also be consulted to examine a particular trace, given that they possess expertise and skills that the criminal investigator lacks, such as forensic physicians and fingerprint experts.

• **Searching for and Hearing Witnesses:**

It is rare, if not impossible, for a crime to be committed without there being any witness. A witness is anyone who perceived the incident through one of his senses, such as seeing the offender while committing the crime or hearing his voice and recognizing him thereby. Among the most important conditions required of witnesses are sanity and maturity. In hearing witnesses, care must be taken not to exert pressure on them, to provide them with the greatest possible degree of psychological comfort, and even to give them guarantees against being harmed by the offender and to protect them, among other measures. The Algerian legislator addressed the methods of hearing witnesses in Section Four, Articles 163 to 174, of Law No. 25-14 dated 03 August 2025, containing the Code of Criminal Procedure.

• **Arresting the Suspect:**

Since arrest affects the human being and one of his most fundamental rights (his liberty), it may not be resorted to except in the case where his commission of a crime punishable by

law is established. This is affirmed by various national legislations, including Algerian legislation, which stipulates in Article 1 of Law No. 24-06 dated 28 April 2024, containing the Penal Code, that: “There is no crime and no punishment or security measure without a law.” It means depriving the accused of his personal liberty for a specific period of time sufficient to investigate him regarding the acts attributed to him. The Algerian legislator addressed the arrest warrant in Article 184 of the aforementioned Code of Criminal Procedure, which is issued by the judge competent to hear the case, and specified its modalities and conditions in Articles 193 to 196 thereof.

- **Search and Seizure:**

Like arrest, search is considered one of the procedures that infringe upon the person, as it primarily concerns his private sanctity, such as his residence, his private means of transportation, or any of his possessions. The primary objective of search is to seize everything related to the crime suspected to have been committed by the person subject to the search. It is one of the most important mechanisms of criminal investigation and may be carried out on the suspect with his consent or without his will. Due to the gravity of search, the law and all legislations have surrounded it with a set of guarantees.

- **Interrogation:**

Interrogation generally aims to obtain information and evidence related to the crime that may assist in uncovering the truth, whether by proving or negating an offense. It refers to hearing the statements of the accused, directing questions to him, and discussing them with him in order to reach the truth regarding the circumstances of the crime. What should be noted here is that interrogation ends with one of two outcomes: either the acquittal of the accused or his confession to what is attributed to him and, consequently, his conviction. In both cases, the investigator has achieved the overall objective of the investigation.[1] the legislator addressed the modalities and conditions of interrogation in Articles 175 to 183 of the aforementioned Law No. 25-14.

b: The Specific Nature of Cybercrime.

There are several names for electronic crime, including computer and internet crimes (Computer crimes), soft crimes (Soft Crimes), and high-tech crimes (High Tech crimes)[2]. This type of crime is committed by accessing electronic communication networks and the private spaces of natural and legal persons. This access, also termed unauthorized intrusion into computer space, falls within the framework of electronic crime.

b-1: Definition of Cybercrime: Doctrinal definitions of cybercrime have varied. Among them is what was presented by the Office of Technology Assessment in the United States, stating that electronic crime is: "crime that

[1] Ibid., p. 95.

[2] Assal, Reda; Abdelrazak, Imad. Cybercrime and the Information Offender: A Conceptual Approach. Bibliophilia Journal for Library and Information Studies, no. 5, 2020, pp. 152–153.

relies primarily on computer evidence and information software[1]".

It was defined by experts from European Union countries as: "any intentional act arising from the unlawful use of information technology and aimed at assaulting material and moral property."[2]

Referring to the Algerian legislator, we find that it did not define electronic crimes clearly but addressed this type of crime through the content of Law 06-23, dated December 30, 2006, amending and supplementing the Penal Code, precisely in Section Seven bis, which it dedicated to offenses against automated data processing systems, enumerating the methods of offenses against automated data processing systems that fall within the scope of electronic crime in Articles 394 bis 1 and 394 bis 2. This was followed by Law 09-04, dated August 5, 2009, containing the Penal Code. Its Article 2 stipulates: "For the purposes of this Law, the following shall mean: ... 1- Offenses against automated data processing systems as defined in the Penal Code and any other crime committed or facilitated through an information system or an electronic communications system..." This is the same approach taken by Article 335 of Law 25-14 when addressing the specialized national penal pole for the prosecution and investigation of crimes related to information and communication technology and associated crimes, defining them as: "any crime committed or facilitated by the use of an information system or an electronic communications system or any other means or mechanism related to information and communication technology."

- **b-2: The Specificity of Cybercrime and Its Reflection on the Difficulty of Detection and Proof:** Examining the characteristics of electronic crimes makes us realize the truth of the difficulty of detecting them, especially when confronting some individuals who possess capabilities in the field of information technology and control over electronic devices.
- **Distinguishing Elements of Cybercrimes:** Cybercrimes involve a high degree of danger to all members of states and are distinguished from other crimes by specific characteristics due to their association with computers and the internet, the most important of which are:
  - **They rely on special methods different from other crimes:** Cybercrime is based on specific methods, capabilities, and practices, such as reliance on intellectual effort. Unlike other crimes, it does not require any physical effort (soft crime) but depends on employing the perpetrator's expertise and ability to deal with the internet.[3]
  - **Speed of execution and the possibility of committing it remotely:** Unlike some other crimes, such as bribery, which sometimes requires the

[1] Qazran, Mostafa; Zarqin, Abdelkader. International Mechanisms for Combating Cybercrime. Sawt Al-Qanoun Journal, vol. 8, no. 2, 2022, p. 1224.

[2] Nashaf, Farid. Mechanisms of International Cooperation in Combating Cybercrimes. Journal of Research in Law and Political Science, vol. 8, no. 1, 2022, p. 432.

[3] Al-Hajini, Munir Mohamed; Al-Hajini, Mamdouh Mohamed. Distribution of Electronic Signature. Dar Al-Fikr Al-Jami'i, Egypt, 2006, p. 112.

presence and meeting of the two parties to the crime (the briber and the bribed), committing a cybercrime does not require the perpetrator's physical presence and can be carried out over large distances. It is quickly executed, as a mere click of a button is enough to execute it.

- **Non-recognition of geographical borders:** The information society is considered open and not restricted to a specific geographical scope. Consequently, information can be exchanged and some transactions conducted between persons separated by thousands of kilometres. As a result, more than one country can be affected in case of conducting illegal transactions and the occurrence of a cybercrime[1].
- **The novelty of electronic crimes and their strong association with internet networks:** Compared to some crimes, cybercrime is relatively recent, due to the means used and the location of its commission (computers and internet networks). Electronic crimes are committed via the internet network as it is the link between the entities targeted by the perpetrators (states, companies, banks, individuals, etc) [2].
- **Difficulty in detecting and proving electronic crimes:** Due to not leaving clear traces, it is difficult to prove the occurrence of this type of crime; hence, some call them hidden crimes. They are also characterized by not being linked to a specific time or place and often go unnoticed until long after their actual occurrence. The foundations upon which crimes are generally based are evidence that condemns the perpetrator and witnesses to the occurrence of the crime, which cannot be achieved with cybercrime. Consequently, the competent authorities find it difficult to accuse the perpetrator of the crime. What is discovered and ascertained of crimes usually happens accidentally and unintentionally. Furthermore, cybercrimes constitute an attractive factor for criminals, especially those proficient in information technology and active in the field of money laundering and theft and sale of various information[3].

2-: Legal Impacts of Technological Development on Investigation Mechanisms: Some consider criminal investigations to be applied sciences concerned with studying tangible facts to prove crimes and the involvement of criminals in committing them. Their means include research, interviewing, interrogation, evidence collection, etc.

a- The Inadequacy of Traditional Procedures in Confronting Digital Evidence: Due to significant developments in the field of criminal investigations, especially with the evolution of crimes and the emergence of new types, such as cybercrimes, which have become difficult to trace through traditional investigation mechanisms previously mentioned, although they cannot be dispensed with

[1] Assal, Reda; Abdelrazak, Imad. Cybercrime and the Information Offender, previously cited, p. 154.

[2] Bounara, Yasmina. Cybercrime. Al-Mi'yar Journal, vol. 40, no. 39, Emir Abdelkader University of Islamic Sciences, 2015, p. 281.

[3] Nashaf, Farid. Mechanisms of International Cooperation in Combating Cybercrimes, previously cited, p. 435.

despite their occasional inadequacy. Among the most important of these mechanisms are the interrogation of witnesses and suspects, collection and seizure of evidence, and collection of documents, papers, and records, conducting searches and forensic medical examinations. These methods often rely on manual examination and practical experiments. In our view, the work or mechanisms used by criminal investigators in criminal investigation, as previously mentioned, can be grouped into two main stages:

a-1: Procedures of the evidence collection and seizure stage: Three procedures can be distinguished in this stage: inspection, examination and expert assistance, and searching for and hearing witnesses.

a-2: Procedures of the search and interrogation stage: This stage comes after sufficient evidence is collected that proves the person's involvement in committing the crime. It encompasses the arrest of suspects, conducting search operations, and

interrogation.

b- The Need for Special Procedural Rules for Digital Investigation: Due to the seriousness and high complexity of cybercrime, it was necessary to find modern mechanisms to keep pace with its repercussions. This is what the Algerian legislator did through Law 09/04 concerning specific rules for the prevention and combating of crimes related to information and communication technology, dated 05/08/2009, as well as Law 25-14 amending and supplementing the Algerian Code of Criminal Procedure by introducing new mechanisms: infiltration, interception of correspondence, electronic surveillance, and preservation and disclosure.

- **Interception of Correspondence:** The Algerian legislator addressed the subject of interception of correspondence in the context of crimes related to information and communication technology, as termed by Law 09-04, and affirmed it under Article 114 of Law 25-14 [1](replacing Article 65 bis 05 of the previous Code of Criminal Procedure). It is an innovative procedure meaning to allow judicial police officers in charge of the case to intercept correspondence conducted through wired and wireless communication means by implementing secret technical arrangements, even without the knowledge and consent of the suspects, where they are eavesdropped on and the necessary data and conversations are captured, recorded, and used as evidence against them. The interception of correspondance process requiers :
  - **Authorization:** It must be written and issued by the competent judicial authorities (the public prosecutor during the preliminary investigation and the investigating judge during the judicial investigation phase) under penalty of nullity of the procedures. It must also include the nature of the crime with a specified

[1] Law No. 25-14 of 9 Safar 1447 AH (corresponding to 3 August 2025), enacting the Code of Criminal Procedure, Official Gazette No. 54, 2025

duration, which is four months, renewable.

- **Reasoning:** It refers to the reasons that necessitated this procedure, which must be substantive and serious.

- **Infiltration and Hacking:** Infiltration, according to Article 121 of Law 25-14, means a member of the judicial police infiltrating the circles of persons suspected of Committing a felony or misdemeanour involving communication and information technology, which constitutes an electronic crime. and deceiving them into believing they are a perpetrator or accomplice with them. For example, this is done by joining them in chat rooms and conversations after hacking their accounts. It can be said to be the most dangerous procedure of all, as it may endanger the infiltrator's life if discovered. Similar to the interception of correspondence, a set of substantive and procedural conditions stipulated in Article 124 of Law 25-14 must be met.

Procedural Conditions: According to the above article, for infiltration to be valid, the following must be available:

Authorization, which must be written, otherwise the procedure is null.

Duration: set at four months, renewable according to the requirements of the investigation and inquiry.

Substantive Conditions: This procedure must meet two basic conditions:

Reasoning: meaning clarifying and explaining the arguments based on which the infiltration authorization was granted, usually for uncovering the crime, its circumstances, and revealing the perpetrators.

Specification of the crime type: This procedure must target a cybercrime.

- **Electronic Surveillance:** Being one of the novel subjects, electronic surveillance was not defined under the aforementioned Law 09-04, which only indicated how to implement it, by putting in place technical arrangements to facilitate the monitoring of electronic communications, according to Article 3 of the same law. It addressed cases of being placed under surveillance in Article 4, paragraph "b," especially in case of a potential threat to state institutions, public order, and the national economy and defence. This is done with a written authorization from the competent judicial authority.

- **Preservation and Disclosure:** Article 10 of Law 09-04 introduced two new procedures: preservation and disclosure. Preservation is done by archiving existing and previously stored data to prevent their damage. With consideration of the time period estimated at one year from the date of recording and the confidentiality of the preservation process, Article 11 of the same law specified the traffic data that service providers are required to preserve upon request from the authorities. These are data that allow the identification of service users, technical characteristics, and the date and duration of communications; data related to requested supplementary services or information used and its provider; data allowing the identification of senders and recipients and their phone numbers and addresses;

data related to equipment used in the communication process.

It must be noted here the necessity of prompt disclosure by service providers of all data that may assist the investigation to the competent authorities, expressed as collecting information, recording it, and making it available to the investigation authority on one hand, and on the other hand, maintaining the secrecy of the operations they perform for those authorities under penalty of the legally prescribed sanctions.

Secondly: Digital Investigation as a Mechanism for Detecting Cybercrimes

Cybercrimes first appeared in developed countries and then in the rest of the world. They are modern crimes that accompanied scientific and technological developments, as previously mentioned, which necessitated finding new ways to try to uncover and decode them. Thus, digital investigation was born, which relies on processing digital data and information to solve the puzzles of crimes.

1- The Legal and Procedural Framework Regulating Digital Investigation: Digital investigation is considered a branch of forensic science. It is a scientific means supporting criminal investigations, aiming to identify, collect, analyse, and present evidence derived from electronic devices to investigators to help reach crime perpetrators and bring them to trial. It primarily focuses on cybercrimes. To achieve tangible results and be able to detect them, a set of controls and conditions must be adhered to when conducting digital investigation, and specific procedures and rules must be followed, which we will try to address in this part of our research paper.

a- Basis for Electronic Search and Seizure: We previously indicated that the primary goal of a search is to seize everything related to the crime and that it is one of the most important criminal investigation mechanisms in general. This was affirmed by the legislator by dedicating a set of legal articles to it in Chapter Three of Law 09-04, mentioned above, namely Articles 05 to 09, listed under the title "Procedural Rules: Searching Information Systems."

a-1: Conditions and Controls for Electronic Search: Searching in electronic crimes does not differ much from traditional searching and occurs according to specific conditions, which can be divided into two parts:

Substantive Conditions: The most important of which are:

Reason for the search: It primarily consists of the occurrence of a cybercrime constituting a felony or misdemeanour, as well as the availability of confirmed indications of the existence of information devices and equipment that could reveal the truth, and the receipt of information indicating the involvement of one or more persons in committing the cybercrime.

- **Subject of the search:** The subject of the search must be a computer with its hardware and software components and the networks connected to it.
- **Authority responsible for the search (investigation authority):** It refers to the authority authorized to

conduct the search. To facilitate the process, it may delegate judicial police officers and agents and any person qualified for that, which is known as delegation.[1]

Formal Conditions: For the search to be valid, a set of formal conditions must be met, the most important of which are:

- **Search warrant:** Issued by the public prosecutor.
- **Presence of the accused:** This is the rule; however, the Algerian legislator deviated from this rule due to the specificity of this type of crime.
- **Timeframes:** Except for exceptional cases, the search is conducted according to general rules at specified times (from 5 am to 8 pm) out of respect for individuals' freedom and rights. However, the Algerian legislator deviated from the general rules in case of a cybercrime due to its nature, allowing judicial police officers to conduct the search at any time by order of the competent investigating judge.[2]
- **Drafting a search report:** This is because the search falls within the investigation process, which requires proving what is discovered in official reports.

a-2: Rules for Digital Seizure and Data Management: We can say that seizure is a procedure connected to and accompanying the search. Conducting a search necessarily means seizing and seizing whatever useful items and information are extracted by taking possession of them to uncover the crime's circumstances and reveal its perpetrators.[3] The seizure of data or information, according to Law 09-04, occurs after the authority responsible for the search discovers useful information stored within an information system. It is not useful to seize it entirely. While respecting the sanctity of others' freedom and ensuring their rights are not violated, that authority or entity is obligated to:

- Copy the requested data or those necessary for understanding them onto a storage medium, according to the provisions of the CPC rules.
- Use necessary techniques to prevent access to data existing in the system or their copying.
- Use necessary technical means and employ qualified persons to prevent access and viewing of data whose content constitutes a crime, to maintain investigation confidentiality.
- Ensure the integrity of the data of the system where the search and seizure operation was conducted.

b- The Probative Force of Electronic Data: The Algerian legislator did not address the definition of digital evidence, neither in Law 09-04 nor in Executive Decree 15-261 regulating the work of the National Authority for the Prevention of Information and Communication Technology Crimes. We note that digital evidence is of great importance in uncovering cybercrimes due to the possibility of using it in investigations, provided that the necessary skills in extracting, analysing, and preserving it are acquired.

---

[1] Majdoub, Nawal. Procedural Mechanisms for Detecting Cybercrime. Journal of Legal and Economic Research, vol. 6, no. 3, 2023, p. 193.

[2] See Article 78 of Law No. 25-14.

[3] See Article 6 of Law No. 09-04 concerning the prevention of information crimes.

b-1: The Legal Nature of Digital Evidence: It can be said that digital evidence is information stored or transmitted in the form of digital data. To understand the legal nature of digital evidence, we will address its definition and clarify its characteristics. Digital evidence can be of a material or immaterial nature, the former referring to any evidence perceivable by the senses.

Definition of Digital Evidence: There are many definitions on the subject, including: Digital evidence is "all data that prove the occurrence of a cybercrime or the existence of a relationship between the crime and the perpetrator or between the crime and the victim. Digital data are the set of numbers representing various information, including written texts, drawings, sound maps, or images."[1]

Some have defined it as: "evidence taken from computer devices in the form of fields or electrical or magnetic pulses that can be collected and their content analysed using special applications and programs so that they can be presented as valid clues for reliance before judicial authorities"[2]

Characteristics of Digital Evidence: Digital evidence is distinguished from other evidence and clues by a set of characteristics, the most important of which are:

- **Digital evidence is scientific evidence:** Unlike ordinary evidence, which is tangible and material through which the perpetrator is reached, electronic (digital) evidence consists of digital data linked to the virtual environment that can only be discovered using complex technical and scientific methods, as it exists in electronic devices such as computers, phones, networks, and differs from traditional material evidence.
- **Digital evidence is technical evidence:** According to the term, digital evidence originates in a digital environment, and therefore it is characterized by a kind of specificity and technical nature, differing from ordinary material evidence in most cases. Consequently, reaching and understanding its content requires great mastery and ability to control various electronic devices by specialists with high technical expertise.
- **Evolution and diversity of digital evidence:** Although the origin of digital evidence is the digital environment and it is fundamentally based on digital computing language, as previously mentioned, this does not prevent digital evidence from being diverse, encompassing all forms of digital data that can be circulated.[3]
- **Difficulty in disposing of digital evidence (Hard to Erase) and its retrievability:** Since digital evidence consists of computer data and information, it is difficult, if not impossible, to dispose of it completely, especially with the development of constantly evolving computer

[1] Abdelkader, Falah; Ait Abdelmalek, Nadia. Criminal Investigation in Cybercrimes and Their Proof in Algerian Legislation, previously cited, p. 170.

[2] Belhadi, Hamid. The Evidentiary Value of Digital Evidence in Criminal Proof. Journal of Legal and Political Research and Studies, vol. 9, no. 1, 2019, p. 16.

[3] Bougassa, Iman. The Impact of the Particularity of Investigation Procedures in Cybercrimes on the Evidentiary Value of Digital Evidence. Journal of Rights and Freedoms, vol. 13, no. 2, 2025, p. 545.

technologies and programs that have become capable of recovering information that has been destroyed or hidden, regardless of its type. This complicates criminals' ability to commit their crimes and contributes to uncovering them, especially if they attempt to erase or hide that data and information, which may be used against them as an additional argument or evidence implicating them[1].

b-2: Conditions for the Admissibility of Digital Evidence before the Court: In addition to being relevant to the incident and documented in an official report, digital evidence must meet a set of conditions to be admissible before the court, the most important of which are lawful collection, reliability, and susceptibility to discussion.

- **Legality:** It means that the digital evidence must be extracted in accordance with the procedures stipulated by law. If those procedures are violated, the digital evidence becomes null and cannot be relied upon, and the person against whom it is used can invoke its nullity.

Examples of illegality include those in charge of the investigation using illegal procedures against a person accused of an electronic crime, such as physical or moral coercion to obtain a specific file or force them to decrypt something, etc. We also face an illegal situation when judicial police officers and their agents conduct eavesdropping or electronic surveillance without permission and authorization from the investigation authority.

- **Certainty (Reliability):** The meaning of this condition is that the content of the digital evidence must be free from speculation and not subject to doubt, especially regarding conviction. Absolute certainty is not required; relative certainty suffices, provided it achieves what is known as the principle of judicial certainty, meaning the evidence carries convincing indicators and clues for all, upon which the judge can base his ruling.[2] Perhaps its collection by specialists and experts in digital evidence collection and examination processes contributes to confirming its reliability.

- **Susceptibility of Digital Evidence to Discussion:** This occurs during the hearing session by discussing the evidence recorded in the case file after the parties have been informed of it. The evidence is presented for discussion and scrutiny before the judge to enable the parties to clarify and object to it.

2- Legal and Organizational Mechanisms Supporting the Effectiveness of Digital Investigation: To achieve the goals of digital investigation and ensure the greatest possible effectiveness, especially in light of electronic crimes transcending state borders, and while considering the rights and freedoms of the persons concerned and respecting its controls, coordination and cooperation between national and international bodies must

[1] Belhadi, Hamid. The Evidentiary Value of Digital Evidence in Criminal Proof, previously cited, p. 20.

[2] Rawabeh, Ilham Shahrazad. Digital Evidence between the Legitimacy of Proof and the Violation of Informational Privacy. Journal of Legal and Political Research and Studies, no. 10, 2022, p. 195.

be ensured to uncover the perpetrators and bring them to trial.

a- Safeguards for Protecting Rights and Freedoms in Digital Investigation: The right to privacy is a constitutionally guaranteed right, falling within the protection of individuals' rights and freedoms. In light of rapid technological development, the emergence of various communication networks, and the circulation and easy accessibility of much information and data, including personal information, and within the framework of the shift towards reliance on digitization in various fields of life, including justice, an urgent need has arisen for mechanisms or safeguards that can protect individuals' rights and achieve what is called secure digital justice that ensures the protection of natural persons in the field of processing personal data under penalty of legal sanctions.[1] This was affirmed by the texts of Law 18-07.[2]

a-1: Protecting Digital Privacy during Search: To achieve greater protection for personal data and prevent infringement of digital privacy, Law 18-07 was enacted, which included a set of articles, in addition to establishing a national authority called the National Authority for the Protection of Personal Data.

- **Meaning of protecting digital privacy:** According to Law 18-07, it means preventing infringement of the rights of natural persons when processing personal data. Protection encompasses any information relating to the data subject, directly or indirectly, such as identity (name, surname, personal address, etc.), physiological makeup and psychological state, financial and social status, and other sensitive data related to their private life. According to paragraph six of Article 03 of the aforementioned law, sensitive data or information means: "**personal data revealing racial or ethnic origin, political opinions, religious or philosophical convictions, or trade union membership of the data subject, or data concerning their health, including genetic data.**"

- **Mechanisms for protecting digital privacy:** By mechanisms here, we mean the rights of the person subject to digital search and the duties of the person conducting it. According to the aforementioned article, the data subject means any natural person to whom the data to be processed relates. The data controller or processor is defined as any natural or legal person, private or public, or any other entity acting alone or with any other person they employ or use in processing the data. To protect the former, the legislator granted them a set of rights, which are considered duties for the latter, summarized as follows:

- **Rights of the data subject regarding the processing of their personal data:** The same law guaranteed every person subject to search or processing of their personal data a set of rights that must be respected, the most important of which are:

[1] See Article 46(4) of Presidential Decree No. 20-442 of 30 December 2020, ratified by referendum on 1 November 2020, Official Gazette of the Algerian Republic, No. 82, amending the Constitution.

[2] See Articles 54, 55, 59, 61, 62, 66, 44, and 67 of Law No. 18-07 of 10 June 2018 concerning the protection of natural persons in the processing of personal data, Official Gazette No. 24, 2018.

• **Informing the data subject of the processing:** With consideration of the procedures and cases stipulated in Article 33 of Law 18-07, every person whose personal data is to be processed, whether contacted for that purpose or not, has the right to know the identity of the data controller or their representative and the purposes used in the operation, along with knowing all additional information such as the recipients and transfer of data to another country and the mandatory nature of the response and its effects. Also, in case their data is collected in an open network without prior knowledge, they have the right to know the possibility of its circulation in that network and that it may be used and accessed by third parties.[1]

• **Ensuring the data subject's right of access:** Article thirty-four of Law 18-07 stipulates the right of the data subject to request from the data controller confirmation as to whether their personal data is being processed or not. Additionally, they have the right to be informed in an understandable manner of the data concerning them undergoing processing, the sources of that data, as well as the justification of the processing purposes and the data concerned.

• **Right to rectification:** Law 18-07 enabled the data subject to request from the data processor to update, correct, delete, or block all data that violates the law's provisions, such as being incomplete, incorrect, or prohibited from processing, within a period of 10 days from notification. In case of the latter's refusal to fulfil their obligations and not responding to the data subject's request within the specified period, the data subject has the right to submit a rectification request to the National Authority, which appoints one of its members to conduct necessary investigations and execute the request. They also have the right to notify third parties to whom the data has been transmitted of the aforementioned, if possible.

• **Right to object:** Unless the processing is in compliance with a legal obligation and provided the reason for objection is legitimate, the data subject has the right to object if the data controller uses those data for advertising purposes, especially commercial ones.

• **Duties of the data processor:** In addition to the rights that must be provided to the data subject, the data processor is obligated to take specific measures to ensure the integrity of the procedure, which are:

• **Taking all necessary measures for the security of data processing:** The data controller processing personal data or any other natural or legal person they employ or delegate a specific task to must take necessary precautionary measures and procedures to protect them from damage or any other threat, such as hacking or unlawful use.[2]

• **Ensuring the confidentiality of processing:** This obligation falls on the data controller as well as every person who has accessed the personal data of the data subject undergoing processing

[1] See Article 32 of Law No. 18-07.

[2] Ben Daas, Siham; Ben Othman, Fawzia. Guarantees for the Protection of Personal Data in the Digital Environment under Algerian Legislation. Journal of Human Rights and Humanities, vol. 15, no. 1, 2020, p. 1691.

or search, such as a subcontractor or any other natural or legal person, private or public, according to Article Three of Law 18-07. We note that this obligation or guarantee continues even after the end of those persons' duties, as they must not disclose anything related to that data, otherwise they are subject to the legally prescribed penalties[1].

- **a-2: Respecting the Principle of Legality and Restricting Investigation Authorities' Powers:** Digital search or processing of personal data is subject to specific controls aimed primarily at protecting digital privacy, which are:

- **Legality:** Whenever we talk about the principle of legality, we refer to Article One of the Penal Code, which stipulates: "No crime, penalty, or security measure without law." From this standpoint, the Algerian legislator emphasized in the texts of Law 18-07 the necessity of adhering to legality during digital search, as addressed in its Article Nine, which states: "...a- Processed lawfully and fairly." From here, we can deduce that the processing of personal data, especially in the digital environment, is subject to respecting the principle of legality. This is done by respecting the legal procedures prescribed for the search and its requirements, such that:

- The collection of personal data aims at specific, clear, and lawful purposes.

- Any subsequent processing of the data is proportionate to the specified purposes and does not deviate from their framework.

- Consent of the data subject to conduct the processing, with consideration of necessary cases where processing of personal data may be conducted without the data subject's consent, where the aforementioned law required obtaining their consent[2] when conducting the operation; thus, the absence of this condition makes the processing operation unlawful.

- **Proportionality:** The collected personal data must be proportionate and not excessive compared to the purpose of their collection, meaning the processing must be based on data directly and closely related to the purposes specified at the beginning of the operation (processing) on one hand, and reasonable and not excessive on the other.[3]

- **Adherence to processing procedures:** The legislator restricted the process of processing personal data by the necessity of taking two prior formal procedures that must be observed before starting the processing, aiming to protect the rights of the data subjects, namely declaration and licensing.

_Prior declaration**:** According to Law 18-07, processing may not be carried out except after obtaining the declaration granted by the National Authority for the Protection of Personal Data. The declaration includes a set of data, the most important of which are: the name of the data processor, the

[1] See Article 40 of Law No. 18-07.
[2] See Article 7(5) of Law No. 18-07.
[3] Ben Daas, Siham; Ben Othman, Fawzia. Guarantees for the Protection of Personal Data in the Digital Environment under Algerian Legislation, previously cited, p. 1683.

nature and characteristics of the processing, its purpose, as well as a description of the data subjects, the recipients, the data retention period, and the authority before which the data subject can lodge a complaint in case of infringement of their rights.

_Licensing**:** The data controller is required to obtain prior licensing if the National Authority, after studying the declaration request submitted by them, determines that there is an apparent risk to the data subject. The National Authority notifies the data controller of the necessity to obtain the license within 10 days from the date of submitting the declaration. We note the possibility of licensing the processing of sensitive information in some cases, especially those related to public interest[1].

Respecting the data retention period: By virtue of this principle, data is retained for a period not exceeding that necessary to achieve the purposes for which it was collected. Accordingly, it is required not to be retained permanently. However, the data retention period may be extended after obtaining permission based on a request from the data controller and for a legitimate interest[2].

b- Institutional and International Cooperation in Digital Investigations: To safeguard the rights of the accused on one hand and to ascertain the true identity of crime perpetrators so that the actual offenders receive appropriate punishment for their actions, national and international efforts in the field of investigation must be intensified.

b-1: Cooperation between Law Enforcement Agencies and Digital Laboratories: Due to the sensitivity of digital investigations and the great importance surrounding them, and in pursuit of uncovering cybercrime perpetrators and achieving the greatest possible deterrence against them, the Algerian legislator mandated and established specific bodies for investigation and providing necessary information to the competent authorities.

Law enforcement agencies:

Preliminary investigation authorities: This investigation, which can be considered a first level of criminal investigation, is exercised by judicial police officers under the supervision of the public prosecution. At this stage, preliminary evidence is collected through interrogation, conducting investigations and inspections, and attempting to reach the perpetrators or at least identify suspects and consider whether there is sufficient evidence to refer them to the competent judicial authorities. This jurisdiction belongs to:

- Judicial police officers mentioned in Article 23 of Law 25-14 containing the Code of Criminal Procedure.
- Employees and agents legally entrusted with some judicial police tasks, specified in Article 29 of Law 25-14.
- Employees and agents charged with some judicial police tasks

[1] See Article 18 of Law No. 18-07.

[2] Ben Daas, Siham; Ben Othman, Fawzia. Guarantees for the Protection of Personal Data in the Digital Environment under Algerian Legislation, previously cited, p. 1684.

according to Article 31 of the Code of Criminal Procedure.

Judicial investigation authorities: Judicial investigation can be considered a second level in the criminal investigation process. At this stage, more evidence and testimonies are generally collected and analysed more deeply and accurately. It is usually exercised by investigating judges and sometimes the indictment chamber (after cases are referred to it).

- **Investigating judge:** After the case file is presented by the judicial police officers (police, gendarmerie, etc.), the role of the competent investigating judge, who is part of the judiciary, comes into play. They examine the accusations brought to them and verify their accuracy, as well as collect evidence for and against. At the end of their investigation, they prepare the case for adjudication according to Articles 139 to 142 or refer its file to the indictment chamber according to Article 262 of Law 25-14.
- **Indictment chamber:** At least one indictment chamber is formed in each judicial council and is considered a second level of judicial investigation, so to speak. Among its tasks is adjudicating what is referred to it by investigating judges, which concerns us in this study. It also undertakes monitoring the work of judicial police officers and agents as well as the work of employees and agents entrusted with some judicial police tasks according to Article 302 of Law 25-14.

Specialized and assisting bodies in investigations: In addition to what the judicial police do, as mentioned above, which has jurisdiction over all crimes, including cybercrimes, as an original jurisdiction, the legislator supported them with new bodies and methods aimed at comprehending everything surrounding this type of crime and attempting to confront them, which are:

- **Regarding the police force:** A central laboratory was established in Châteauneuf, Algiers, and two regional centres in the states of Constantine and Oran. They include technical branches, including the computer unit and specialized teams tasked with investigating and detecting internet crimes. The scientific police laboratories of Constantine and Oran also contain two special laboratories tasked with investigating electronic crime, named "Digital Evidence and Technological Traces Division."
- **Regarding the National Gendarmerie:** The National Gendarmerie exercises its tasks of confronting electronic crime through two bodies: the General Directorate of Security and Exploitation and the Central Service for Criminal Investigations, which is a body with national jurisdiction, in addition to the National Institute of Forensic Evidence and Criminology, which follows the IT and Electronics Department of the Gendarmerie General Command.[1]
- **Centre for the Prevention of Computer and Electronic Crimes:** It

[1] Abdelkader, Falah; Ait Abdelmalek, Nadia. Criminal Investigation in Cybercrimes and Their Proof in Algerian Legislation, previously cited, p. 196.

is a national body whose establishment was stipulated by Article 13 of Law 09-04, generally entrusted with coordinating and stimulating operations for the prevention and combating of crimes related to information and communication technology, in addition to assisting judicial authorities and judicial police services in investigations, as well as external coordination, exchange of information, and collection of data aiding in identifying electronic crime perpetrators. It should be noted that the composition, organization, and operating procedures of this body were specified by Presidential Decree 15-261[1].

- **Service providers:** The diversity of services provided in the field of information and communication technology requires the existence of operators whose task is to provide and supply those services. The legislator addressed this category in Article 10 of Law 09-04, obligating them to provide necessary assistance to the competent authorities in the field of immediate reporting and preservation of data related to communication content and not disclosing information about the operations they perform for those authorities.

b-2: Mechanisms of International Cooperation and Information Exchange: We can distinguish two aspects or mechanisms of international cooperation in the field of combating cybercrimes: procedures of a technical nature aimed at preventing the crime during its execution, called security cooperation; and cooperation for law enforcement and prosecution and punishment of electronic crime perpetrators, which comes after their commission and consists of judicial cooperation[2].

- **Security cooperation:** After practice proved the inability of states individually to combat this type of crime due to its specificities, it was necessary to find ways to achieve that. From this perspective, the need arose to establish international organizations within which states' specialized police agencies operate and exchange information and data to the extent that ensures faster and more effective crime fighting, the most important of which are Interpol and the International Web Police.

International Web Police: This organization was established in the USA in 1986 and was entrusted with the task of receiving complaints filed by network users and pursuing hackers and perpetrators of internet crimes. It consists of specialists, police officers, and technical volunteers.

_International Criminal Police Organization (Interpol): Established in 1923 in Vienna, Austria, it is the largest communication network for exchanging information between police members of member states. Article Two states the pursuit of some objectives, the most important of which are:

[1] Presidential Decree No. 15-261 of 24 Dhu al-Hijjah 1436 (corresponding to 8 October 2015), determining the composition, organization, and operating procedures of the National Authority for the Prevention and Combating of Crimes Related to Information and Communication Technologies, Official Gazette No. 53, 2015.

[2] Nashaf, Farid. Mechanisms of International Cooperation in Combating Cybercrimes, previously cited, pp. 437–439.

- Cooperation among member states in apprehending fugitives and wanted persons, regardless of their nationalities, upon issuance of judicial rulings against them or warrants for their appearance before judicial authorities for investigation.
- Supporting police efforts in combating cross-border crime and providing some assistance services to reach offenders, such as fingerprints and DNA.
- Collecting information related to crimes and criminals obtained from national police central offices at the headquarters.
- Affirming and encouraging mutual assistance on the widest scale between criminal police authorities within the limits of the laws in force in the states and being guided by the Universal Declaration of Human Rights.
- Establishing and developing systems that effectively and efficiently contribute to preventing and combating crimes under common law[1].

Judicial cooperation:[2] Judicial cooperation takes several forms, the most important of which are mutual legal assistance, letters rogatory, and transfer of proceedings.

_Mutual legal assistance: It is one of the most important international mechanisms in combating cybercrime and among the most effective in tracking its perpetrators and punishing them. Article 25 of the 2001 Budapest Convention on Cybercrime addressed the provisions of mutual legal assistance in the field of combating those crimes. Mutual legal assistance is only achieved with the availability of three steps:

- Request**:** Submitted by the state with criminal jurisdiction for prosecution, subject to the law of the requesting state and within the framework of the agreement concluded with the state providing assistance.
- Examination of the request**:** Conducted by the state that will provide assistance, by verifying that the incident concerned by the request is considered a crime according to the law of the requesting state, provided it falls within the jurisdiction of the requested state and according to what is agreed upon between the two states.
- Execution of mutual legal assistance**:** Executed according to the rules of the requested state.

_Transfer of proceedings: It means a specific state taking criminal proceedings regarding a crime committed in the territory of another state and for the benefit of that state. It occurs with the availability of conditions, the most important of which are: The act attributed to the person is considered a crime in both states. The proceedings requested to be taken are provided for in the law of the requested state for the same crime. The procedure leads to reaching the truth.

_Letters rogatory: It means a request to take a specific procedural action in criminal proceedings aimed at considering a matter presented before the judicial authority of the requesting state. It is submitted to the requested

[1] Kharashi, Adel Abdel Aal Ibrahim. Issues of International Cooperation in Combating Information Crimes and Ways to Overcome Them. Faculty of Sharia and Law, Cairo, pp. 195–197. (Available at: https://jfslt.journals.ekb.eg/article)

[2] Ibid., p. 199.

state when the requesting state is unable to perform it itself.

Conclusion

In conclusion, we note that despite the possibility of relying on them sometimes, given the significant role they play in uncovering various crimes, traditional methods have become clearly inadequate in facing cybercrimes, which are evolving continuously and rapidly, making them difficult to contain and confront.

We also point out that the Algerian legislator adopted the principle of freedom of criminal proof enshrined in Article 349 of the Algerian Code of Criminal Procedure, which is the basis upon which the trial judge builds their ruling, having the freedom to choose whatever evidence presented before them. Accordingly, the judge may disregard the results of digital investigations based essentially on digital evidence.

We also observe the reality of scarce international cooperation in the field of combating electronic crimes, which facilitates criminals escaping punishment, especially in light of conflicting interests between some states and some of them harbouring some criminals to serve certain agendas under various guises, such as political asylum.

Therefore, we propose some mechanisms that we believe could contribute to confronting cybercrimes, which are:

- Intensifying training courses for those conducting investigations in the field of cybercrimes to enable them to keep pace with continuous developments and updates, as well as providing them with modern means and techniques and training them on how to use them so they can confront this type of crime more effectively.
- Activating the role of bodies and authorities mandated to combat electronic crimes, including the National Authority for the Protection of Personal Data.
- Intensifying international cooperation in the field of combating cybercrimes that harm the international community as a whole.
- Giving greater value to digital evidence, which is the basis for uncovering cybercrimes, and proposing enacting laws regulating it and making it one of the tools relied upon in proof, especially in light of the freedom judges enjoy in using them as evidence upon which rulings are based or not.

References .

1. Abdelkader, Falah, and Nadia Ait Abdelmalek. Criminal Investigation in Cybercrimes and Their Proof. Al-Ustadh Al-Baheth Journal for Legal and Political Studies 4, no. 2 (2019): 1695–1700.

2. Arabi, Ahmed. Criminal Investigation. 1st ed. Dubai: Dubai Police Academy, 2021.

3. Assal, Reda, and Imad Abdelrazak. Cybercrime and the Information Offender: A Conceptual Approach. Bibliophilia Journal for Library and Information Studies, no. 5 (2020): 152–154.

4. Belhadi, Hamid. The Evidentiary Value of Digital Evidence in Criminal Proof. Journal of Legal and Political Research and Studies 9, no. 1 (2019): 16–20.

5. Ben Daas, Siham, and Fawzia Ben Othman. Guarantees for the Protection of Personal Data in the Digital Environment under Algerian Legislation. Journal of Human Rights and Humanities 15, no. 1 (2020): 1683–1691.

6. Bounara, Yasmina. Cybercrime. Al-Mi'yar Journal 40, no. 39 (2015): 281.

7. Bougassa, Iman. The Impact of the Particularity of Investigation Procedures in Cybercrimes on the Evidentiary Value of Digital Evidence. Journal of Rights and Freedoms 13, no. 2 (2025): 545.

8. Kharashi, Adel Abdel Aal Ibrahim. Issues of International Cooperation in Combating Information Crimes and Ways to Overcome Them. Cairo: Faculty of Sharia and Law, n.d.

9. Majdoub, Nawal. Procedural Mechanisms for Detecting Cybercrime. Journal of Legal and Economic Research 6, no. 3 (2023): 193.

10. Naji, Yaacoub, and Abdel Rahman Othmani. Criminal Investigation and Inquiry through Traditional Methods. Journal of Legal Studies 7, no. 2 (2020): 527–529.

11. Nashaf, Farid. Mechanisms of International Cooperation in Combating Cybercrimes. Journal of Research in Law and Political Science 8, no. 1 (2022): 432–439.

12. Qazran, Mostafa, and Abdelkader Zarqin. International Mechanisms for Combating Cybercrime. Sawt Al-Qanoun Journal 8, no. 2 (2022): 1224.

13. Rawabeh, Ilham Shahrazad. Digital Evidence between the Legitimacy of Proof and the Violation of Informational Privacy. Journal of Legal and Political Research and Studies, no. 10 (2022): 195.

14. Salama, Mamoun Mohamed. Criminal Procedure in Egyptian Legislation. Vol. 1. Cairo: Dar Al-Nahda Al-Arabiya, 2008.

Legal Texts

15. Algeria. Law No. 09-04 concerning the Prevention of Information Crimes.

16. Algeria. Law No. 18-07 of 10 June 2018 on the Protection of Natural Persons in the Processing of Personal Data. Official Gazette No. 24 (2018).

17. Algeria. Law No. 25-14 of 3 August 2025 enacting the Code of Criminal Procedure. Official Gazette No. 54 (2025).

18. Algeria. Presidential Decree No. 15-261 of 8 October 2015 establishing the National Authority for the Prevention and Combating of ICT-Related Crimes. Official Gazette No. 53 (2015).

19. Algeria. Presidential Decree No. 20-442 of 30 December 2020 amending the Constitution. Official Gazette No. 82 (2020)