



Legal Value Of Forensic Digital Evidence -Between The Requirements Of The Legal Text And The Demands Of The Digital Environment

Ali GHRIBI *

Research Center for Islamic Sciences
and Civilization, Laghouat, Algeria,
a.ghribi@crsic.dz

Send Article Date: 06-02-2025

Date of acceptance of the article: 19-05-2025

Abstract:

This research paper aims to address the legal value of digital forensic evidence and the legal and technical problems , it raises at the same time, as despite the positive role that Digital media plays in all areas of life, it negatively affects the increase in crime rate, the diversity of its methods, and building a generation of Criminals who specialize in information technology and the use of modern technology, so that the crime is no longer difficult or high risk, and the disappearance of barriers between countries, cultures and languages contributed to this, and the complete openness that allows the exchange of information easily.

key words: legal value, digital forensic evidence, legal texts.

Introduction:

The evidence of proof came as a result of practical reality and an expression of what individuals have become accustomed to in their transactions, and the legislator did not impose it on them, but rather was satisfied with organizing and approving this evidence. Individuals have become accustomed to using paper bonds to prove their actions due to their confidence in these bonds, as they are evidence that is characterized by stability and

* Ali Ghribi



.....

is difficult to tamper with or forge in a hidden manner, as it is easy to discover this through the apparent view of the bond or its examination by experts specialized in proving the validity of bonds. Therefore, the evidence of proof, for many years, has been proceeding within a closed legal framework, in which this evidence was included exclusively, and accordingly, the law is the one that determines its strength in proving legal actions, and the judge must base his conviction in light of that evidence specified by the law, so the evidence he obtains through his emotional conviction is not taken into account if the law has not stipulated it (Abbas Al-Aboudi ,2010, p08).

However, traditional evidence, especially paper bonds, has been greatly shaken by the emergence of electronic bonds, as a result of the increasing development of modern technology and its dominance over all aspects of contemporary life, including the legal aspect (Muhammad Hussein Mansour 2004, p275).

The English professor Robin Widson points out that the future of electronic bonds extracted from instant communication means will occupy a prominent and important role, not only among individuals, but will also affect the work of the courts and help them in adding a rational character to the administration of justice and its smooth running(Robin Widson, 1997, p 143).

There is no doubt that the information revolution has left positive effects and constituted a qualitative leap in the lives of individuals and countries, due to its speed and accuracy in collecting, storing and processing information. However, this aspect and the positive effects it has left do not negate the negative aspects it has produced, which are mainly represented in the emergence of new crimes that were not known before, and many researchers and specialists have agreed to call them information or digital crimes, which have now become a threat to the interests of individuals and countries in all fields. To combat information crime, it has become necessary to find new means that are radically different from what is used in combating ordinary crime, due to the inability of traditional investigation

procedures to keep pace with the development of this crime, in addition to the inability of physical forensic evidence to prove its occurrence, which required the investigation authorities to rely on a new type of forensic evidence in the field of forensic evidence known as digital forensic evidence.

Based on the above, we decided in this research paper to address the legal value of digital forensic evidence by raising a central problem lies in determining the legal weight to be afforded to digital forensic evidence, given the inherent challenges of reconciling traditional legal frameworks with the unique characteristics of the digital environment. To answer this problem, we divided this research paper into two sections They will be discussed as follows.

SECTION I: CONDITIONS FOR THE JUDICIAL ACCEPTANCE OF DIGITAL FORENSIC EVIDENCE IN CRIMINAL CASES

Digital forensic evidence is a branch of forensic science that deals with searching for data stored in electronic devices, obtaining, processing, analyzing and reporting it. Electronic evidence constitutes one of the components of almost all criminal activities, and it is of great importance to support investigations conducted by law enforcement agencies in the field of digital forensic evidence. This evidence can be collected from various sources such as computers, smartphones, remote storage devices, drones, equipment carried on ships, and others (Ali Ghribi, 2018, p4).

The primary objective of digital forensic evidence is to extract data from electronic sources, process that data, and transform it into actionable intelligence for investigative or legal purposes, and present the results in the context of judicial prosecutions. Sound techniques in the field of forensic evidence are used in all these processes to ensure that the results are accepted in court. The mere existence of evidence proving the occurrence of a crime and attributing it to a specific person is not sufficient to



.....

rely on it to issue a conviction, as this evidence must have legal value(Khaled Ayyad Al-Halabi,2020, p 235), and this value depends on its submission to the rules established in criminal evidence, and this is also the case for digital criminal evidence, which must also be subject, like other evidence, to the rules of criminal evidence, in that the evidence must be characterized by legitimacy, and must also be certain in its indication of the facts to be proven, and finally be subject to discussion. Accordingly, in this section, we will address the conditions for accepting digital criminal evidence before the criminal judiciary through:

First requirement: The legal basis for the recognition of digital evidence in criminal proceedings

The principle of evidentiary legitimacy mandates that judicial convictions be grounded solely upon valid and legally admissible evidence (Nasreddine Marouk, 2003, p519), through the necessity of the procedure being consistent with the legal rules and established systems of society. The aim of this is to establish the basic guarantees for individuals and protect their freedoms and personal rights from the arbitrariness of the investigating authority in cases other than those permitted by law (Kamal Muhammad Awad, 2011, p165).

The principle of evidentiary legitimacy in criminal proceedings extends beyond mere adherence to legislatively enacted rules. While compliance with statutory provisions is a necessary condition, it is not sufficient. The legitimacy of criminal evidence must also be evaluated in light of broader human rights declarations and principles. This means that evidence, even if technically compliant with domestic legal rules, may be deemed illegitimate if its acquisition or use violates fundamental human rights.

For example, evidence obtained through torture, coercion, or illegal searches and seizures, even if admissible under a narrow interpretation of domestic law, would likely be considered illegitimate under international human rights standards. Therefore, assessing the legitimacy of criminal evidence requires

a dual analysis: first, conformity with specific legal rules, and second, compatibility with overarching human rights principles. This ensures that the pursuit of justice is not achieved at the expense of fundamental rights and freedoms. The judge, in evaluating the admissibility and weight of evidence, must consider both aspects, ensuring that the evidence not only complies with legal technicalities but also respects fundamental human rights., international charters and agreements, and public order rules must also be taken into account (Ahmed Abdel-Lah Hilali,, 2004, p 429).

The legitimacy of existence means that digital criminal evidence is recognized, meaning that the law allows the judge to rely on it to form his belief in the conviction ruling (Khaled Ayyad Al-Halabi,2020, p 236).

the legal status and admissibility of digital criminal evidence are inextricably linked to the nature of the prevailing evidentiary system within a particular jurisdiction.

Different countries adopt varying approaches to the reception and evaluation of evidence, and these differences significantly impact how digital evidence is treated. Some jurisdictions may embrace a more liberal approach, readily admitting digital evidence subject to basic authentication and relevance checks. Others may adhere to stricter standards, demanding rigorous chain of custody documentation, specialized forensic analysis, and adherence to specific procedural safeguards. The rules governing admissibility may address various aspects of digital evidence, including its collection, preservation, analysis, and presentation in court. These rules might specify requirements for warrant procedures, data integrity, forensic tool validation, expert witness testimony, and the burden of proof. Furthermore, the weight afforded to digital evidence may also vary depending on the jurisdiction and the specific type of digital evidence in question. For instance, some types of digital evidence, such as metadata or log files, might be considered less reliable than other forms, such as data extracted directly from a hard drive. The legal framework may



also address emerging challenges posed by new technologies, such as cloud computing, encryption, and mobile devices. In jurisdictions with more traditional evidentiary rules, adapting these rules to accommodate the unique characteristics of digital evidence can be a complex and evolving process. Judges may need to grapple with issues such as data volatility, ease of alteration, and the potential for bias in forensic tools.

Ultimately, the legitimacy and probative value of digital criminal evidence are determined by the interplay between the specific legal rules of evidence in a given country and the evolving understanding of digital technology and its forensic applications.

Paragraph 1: Legality of digital evidence in restricted systems

Based on this system, the legislator is the one who exclusively determines the criminal evidence that the judge may resort to in proof, and also determines the persuasive force of each criminal evidence (Khaled Ayyad Al-Halabi, 2020, p 236), the judge's role in a legal proceeding is fundamentally defined by the principle of judicial impartiality and adherence to the rule of law. This role is not one of active investigation or advocacy, but rather one of judicious assessment and application. The judge's primary responsibility is to act as a neutral arbiter, ensuring that the proceedings are conducted fairly and in accordance with established legal principles and procedures.

In the context of evidence, the judge's function is specifically circumscribed. The judge does not gather evidence independently. Instead, the parties to the case present evidence, and the judge's role is limited to:

1. **Examining the evidence presented:** This involves carefully considering the nature, relevance, and probative value of each piece of evidence. The judge must assess the credibility of witnesses, scrutinize documents, and evaluate the reliability of any other form of evidence presented.

2. **Ensuring compliance with legal requirements:** The judge must ensure that all evidence presented adheres to the rules of evidence established by law. This includes determining whether evidence was obtained legally and ethically, whether it is relevant to the case at hand, and whether it satisfies any specific evidentiary standards or thresholds.

The judge's role is not to determine the truth of the matter directly, but rather to ensure that the decision-making process is based on evidence that is both credible and legally admissible. By adhering to these principles, the judge safeguards the integrity of the legal process and upholds the fundamental principles of justice and fairness.

This formulation emphasizes the judge's role as a neutral arbiter and highlights the limitations of their involvement with evidence. It also underscores the importance of adhering to legal rules and principles in evaluating evidence.

Accordingly, there is no way to rely on any evidence that the law has not explicitly stipulated within the evidence of proof. In Britain, for example, which adopts the restricted (legal) evidence system, the Police and Criminal Evidence Act was issued in 1984, which contained a specific regulation of the issue of accepting digital criminal (Ali Hassan Mohammed Al-Tawalbeh, 2004, p. 196) evidence in its various forms as evidence of proof in criminal cases.

Paragraph 2: The legal standing of digital evidence within a free evidentiary framework

According to this system, the judge enjoys absolute freedom regarding the proof of the facts presented to him, because the law does not oblige him to form his conviction with specific criminal evidence, but he can rely on any criminal evidence he deems appropriate, even if it is not stipulated by law (Khaled Ayyad Al-Halabi, 2020, p 237).

In a legal system that operates under the principle of free proof in criminal matters, the question of the inherent legitimacy of



.....

digital forensic evidence largely becomes moot. Because the legislator in such a system is not obligated to enumerate or define specific forms of admissible evidence, the foundational premise shifts. Instead of pre-defined categories of permissible evidence, the default position becomes the general admissibility of any evidence deemed relevant and probative by the court. Therefore, the mere existence of digital forensic evidence, provided it is relevant to the case at hand, does not typically raise a threshold issue of legitimacy. The focus shifts from categorizing the evidence to evaluating its reliability, relevance, and probative value. In essence, under a free proof system, the "existence" of evidence, including digital evidence, is not the primary legal hurdle. The critical considerations become whether the evidence is authentic, whether it has been tampered with, whether it is relevant to the facts in issue, and ultimately, whether it is persuasive to the trier of fact. This framework does not preclude challenges to digital evidence, but the challenges would likely center on these factors (authenticity, integrity, relevance, and probative value) rather than on a categorical exclusion of digital evidence as a type of evidence. The judge retains the discretion to weigh the evidence and assess its credibility, but the fundamental principle of free proof removes the initial barrier of establishing the inherent legitimacy of a particular form of evidence, including digital evidence. (Khaled Ayyad Al-Halabi, 2020, p 238), which is the same as what the Algerian and French legislators have tended towards, considering that they adopt the free evidence system.

Second requirement: The legitimacy of obtaining digital forensic evidence

The talk about the legitimacy of obtaining forensic evidence is always associated with the necessity of protecting and respecting human rights, considering that all legal procedures aimed at obtaining forensic evidence affect the rights and freedoms of individuals, and among these rights is the right to privacy, so taking the measure of electronic surveillance or intercepting

correspondence undoubtedly represents an attack on private life, which has made it a subject of great interest by international declarations and conventions (Moatasem Khamis Mshasha, 2013, p 34), A clear illustration of this principle can be found in Article 12 of the Universal Declaration of Human Rights, which explicitly protects individuals from arbitrary interference with their privacy, family, home, or correspondence, and from attacks upon their honor and reputation. This article affirms that "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." This declaration underscores the fundamental right to privacy and the corresponding obligation of states to provide legal recourse against violations of this right .

On the other hand, and in line with the international trend in recognizing and protecting this right, many legislations, including Algerian legislation, have emphasized the right to privacy and its protection, The constitutional protection of privacy and correspondence is explicitly enshrined in Article 47 of the 2020 constitutional amendment. This article establishes a dual guarantee, encompassing both a general right to privacy and a specific right to confidentiality of communications.

Firstly, Article 47, paragraph one, affirms the fundamental right of every individual to the protection of their private life and honor. This broad provision recognizes the inherent dignity and autonomy of each person and safeguards their personal sphere from unwarranted intrusion. It encompasses a range of protections, including the right to control access to one's personal information, the right to respect for one's family life, the right to bodily integrity, and the right to freedom from defamation. This protection extends to all aspects of an individual's private life, including their personal relationships, health, finances, and personal beliefs.



.....

Secondly, and building upon this general right to privacy, Article 47, paragraph two, explicitly guarantees the confidentiality of correspondence and private communications, "in any form." This provision recognizes the particular sensitivity of private communications and seeks to protect them from unauthorized access or disclosure. The phrase "in any form" is particularly significant, as it demonstrates a clear intent to extend this protection to all forms of communication, regardless of the technology used. This includes traditional forms of correspondence, such as letters and telegrams, as well as modern digital communications, such as emails, text messages, and online chats. The inclusion of this broad language ensures that the constitutional protection of communication confidentiality remains relevant and effective in the face of rapidly evolving technologies. This explicit protection of private communications reinforces the broader right to privacy and underscores the importance of safeguarding personal communications from arbitrary interference. The combined effect of these two paragraphs of Article 47 is to create a robust constitutional framework for the protection of privacy and confidentiality in Algeria, and the legal protection of this right stipulated in the Constitution comes through the Penal Code, as stated in the text of Article 303 bis of the Penal Code (Order No. 66-156 dated 06/08/1966 including the Penal Code, Official Journal No. 49, issued on 11/06/1966 Amended and supplemented), The Algerian legislature reinforces the constitutional guarantees of privacy and confidentiality through specific penal provisions. A clear example of this is the law that criminalizes intentional violations of private life, specifically targeting unauthorized capture, recording, or transmission of private or confidential calls or conversations. This law stipulates that "Anyone who intentionally violates the sanctity of the private life of persons, and by any special technology, by capturing, recording or transmitting private or confidential calls or conversations without the permission or consent of their owner shall be punished with

imprisonment from six months to three years and a fine of 50,000 Algerian dinars to 300,000 Algerian dinars." This provision demonstrates a clear commitment to protecting individuals from technological intrusions into their private communications and underscores the seriousness with which such violations are regarded. The inclusion of the phrase "by any special technology" is particularly noteworthy, as it reflects an awareness of the evolving nature of surveillance technologies and a desire to ensure that the law remains applicable to new and emerging methods of intrusion. This specific criminal sanction complements the broader constitutional protections enshrined in Article 47, providing a concrete mechanism for enforcement and deterrence.

Historically, the French legislator has been at the forefront of efforts to protect private life. This commitment is evidenced by the enactment of Law No. 70-643 dated July 17, 1970, which marked a significant early step in legally safeguarding individual privacy. Furthermore, Law No. 78-17, enacted in 1978 and concerning the electronic processing of official data, further solidified these protections. This later law specifically included provisions for the protection of personal data relating to the private lives of individuals, recognizing the increasing vulnerability of personal information in the context of computerized data processing. These legislative initiatives demonstrate a long-standing recognition in French law of the importance of protecting individual privacy, particularly in the face of technological advancements that can pose new threats to this fundamental right. The French approach highlights the ongoing evolution of legal protections for privacy, adapting to new challenges posed by technological developments (Susan Adnan Al-Ustadh, 2013, p 437), in addition to what the French Penal Code stipulated by criminalizing many acts that affect personal electronic data, such as what was stipulated in Article 226 bis 1, which punishes anyone who electronically processes personal data without a license, as well as what was stipulated in Article



226 bis 21, which punishes deviation from the purpose of electronic processing of personal data.

Therefore, based on the above, both Algerian and French legislators were keen to protect the individual's private life, by raising the status of this right and placing it among constitutional rights, in addition to establishing penalties for all acts that violate it, but this does not mean that this right cannot be violated at all, as the law has set exceptions to this constitutional rule, by allowing this right to be violated if necessary (The principle of protecting private communications, while fundamental, is not absolute. Recognizing that certain overriding societal interests may necessitate limited exceptions, the Algerian legislator has provided for such exceptions within the legal framework. Article 3 of Law 09-04, dated August 16, 2009, concerning special rules for the prevention and combating of crimes related to information and communication technologies, articulates a clear and specific exception to the general rule of confidentiality. This article states that: "Taking into account the legal provisions that guarantee the confidentiality of correspondence and communications, the requirements of protecting public order or the requirements of ongoing judicial investigations or inquiries, in accordance with the rules stipulated in the Code of Criminal Procedure and in this law..." This provision carefully balances the protection of individual privacy with the legitimate needs of law enforcement and national security. It establishes that intrusions into private communications may be permissible under strictly defined circumstances, namely when necessary to protect public order or when required for ongoing judicial investigations or inquiries. Importantly, this exception is not a blanket authorization for unrestricted surveillance. Rather, it is explicitly conditioned upon adherence to the rules and procedures stipulated in the Code of Criminal Procedure and Law 09-04 itself. This ensures that any intrusion into private communications is subject to legal safeguards and oversight, preventing arbitrary or abusive use of these exceptional powers. The inclusion of these procedural

safeguards underscores the legislature's intention to limit the scope of the exception and to ensure that it is only invoked when absolutely necessary and in accordance with established legal processes. This carefully crafted exception demonstrates a nuanced approach to balancing individual rights with societal needs, recognizing that while privacy is a fundamental right, it may be subject to carefully circumscribed limitations in specific and justifiable circumstances, may establish technical arrangements to monitor electronic communications and collect and record their content in a timely manner and carry out inspection and seizure procedures within an information system."), by carrying out procedures to inspect computer systems or monitor electronic communications in order to extract digital criminal evidence, provided that the procedures specific to them and stipulated by law are respected.

On this basis, and within the framework of the legitimacy of obtaining digital criminal evidence, the French legislator, although it did not include The pursuit of truth in criminal justice systems is fundamentally intertwined with the principles of honesty and integrity. While no single legal text may explicitly codify a broad "principle of honesty and integrity in the search for truth," this principle is woven throughout legal frameworks and is implicit in the ethical obligations of all participants in the criminal justice process. It is a foundational value that underpins the admissibility and evaluation of evidence, the conduct of investigations, and the integrity of judicial proceedings.

Although a single, comprehensive article may not exist explicitly stating this principle, its essence is reflected in various legal provisions and ethical codes. For example, laws regarding perjury and false testimony directly address dishonesty in providing evidence. Rules governing the admissibility of evidence, particularly those concerning illegally obtained



.....

evidence or coerced confessions, implicitly uphold the principle of integrity by excluding evidence obtained through dishonest or unethical means.

Furthermore, professional codes of conduct for lawyers, judges, and law enforcement personnel emphasize honesty, integrity, and objectivity in the performance of their duties. These codes often include provisions related to the proper handling of evidence, the avoidance of conflicts of interest, and the duty to act in the interests of justice.

Jurisprudence and judicial practice have further solidified this principle. Courts regularly scrutinize the methods by which evidence is obtained, ensuring that it has not been tampered with or obtained through deception. Judges instruct juries to consider the credibility of witnesses and the reliability of evidence, implicitly emphasizing the importance of honesty and integrity in the fact-finding process. Appellate courts often overturn convictions based on evidence obtained improperly, underscoring the judicial commitment to ensuring that the pursuit of truth is not compromised by dishonest or unethical practices. In essence, the principle of honesty and integrity in the search for truth, though perhaps not explicitly stated in a single text, is a fundamental and pervasive value that shapes the entire criminal justice system, informing legal rules, ethical obligations, and judicial decision-making (Ali Hassan Muhammad Al-Talaba, p187), such that the use of modern scientific methods in searching and extracting criminal evidence, including digital evidence, was accepted under the condition that it be obtained in a legitimate and honest manner. The second section: The judge's powers in assessing digital criminal evidence (Ahmed Abdel-Lah Hilali, p753).

The greatest responsibility of the judge is to assess the evidence and be convinced of it, so that no innocent person is convicted and no criminal escapes. Before issuing his ruling, the judge searches for the truth (Ali Ghribi, p 10).

To do so, he examines the criminal evidence and presents it in the session for the opponents to examine in an effort to reach the

truth that satisfies his conscience and forms his personal conviction to achieve justice. Accordingly, the criminal judge's powers in assessing the evidence differ from one country to another according to the evidence systems that each country adopts. According to what comparative historical studies have revealed in this field, there are two systems: the restricted (legal) evidence system and the free evidence system. In this section, we will discuss the position of the French and Algerian legislators on the judge's powers in assessing digital criminal evidence through legal texts.

first requirement: The position of French legislation on digital forensic evidence

French legislation is considered one of the first legislations to adopt the free evidence system, according The French Code of Criminal Procedure, in Article 427, articulates a principle of broad admissibility of evidence, stating: "Crimes may be proven by all means of proof unless the law provides otherwise, and the judge rules according to his personal conviction." This article establishes a foundational principle of "free proof" (sometimes referred to as "moral certainty") in criminal proceedings. It signifies that, in principle, any type of evidence can be used to establish guilt or innocence, provided it is relevant and probative. The crucial caveat, "unless the law provides otherwise," acknowledges that specific legal rules may restrict or exclude certain types of evidence (e.g., illegally obtained evidence, privileged communications). This caveat ensures that the broad principle of admissibility does not override other fundamental legal principles or protections.

The second part of Article 427, "and the judge rules according to his personal conviction," is equally important. It underscores the judge's central role in evaluating the evidence and forming their own "in time conviction" (personal conviction) regarding the guilt or innocence of the accused. This does *not* mean that the judge's decision is arbitrary or based on whim. Rather, it signifies that the judge, after carefully considering all the evidence



.....

presented, must reach a subjective, reasoned belief about the facts of the case. This conviction must be based on the totality of the evidence and must be justifiable. The judge cannot simply rely on intuition or conjecture; their decision must be grounded in the evidence presented at trial. This principle recognizes the inherent limitations of any evidentiary system and places a significant responsibility on the judge to weigh the evidence fairly and impartially, ultimately forming a reasoned and justifiable conviction. Article 427, therefore, establishes a framework where a wide range of evidence is admissible, but the judge plays a critical role in assessing its value and forming a reasoned judgment, and also Article 304 of the same law states that: "... the jurors swear to issue their decisions according to their consciences and personal conviction"..., and thus the principle of the judge's personal conviction extends to include all criminal judicial bodies (the misdemeanor and contravention court and the criminal court) and also includes all stages of the public lawsuit.

Speaking about the position of the French legislator on digital forensic evidence, it can be said that this type of evidence does not pose any difficulty as long as the legislator adopts the free evidence system, whether it is related to the extent of freedom to present this evidence to prove the cybercrime, or the extent of the judge's freedom to assess it (Ahmed Abdel-Lah Hilali, p721), which is the opposite of legislation that adopts the restricted (legal) evidence system such as England, which obligated respect for the methods of presenting digital forensic evidence and subjecting it to confidence tests(Peter Sommer, 2011. p 80).

In addition, French jurists are studying the issue of accepting digital forensic evidence before criminal courts within a broader scope, which is the issue of accepting evidence resulting from electronic devices other than computers, such as evidence resulting from cameras, surveillance cameras, radars, audio recording devices, etc. Therefore, the French Court of Cassation ruled in a decision issued on 28/04/1987 that magnetic recording

tapes that have evidentiary value can be valid for presentation before criminal judiciary.

Accordingly, electronic audio recording by means of special devices does not tolerate error and is difficult to tamper with, and technical experts can discover any tampering or attempt to destroy it by means of highly efficient technical means. Likewise, evidence resulting from computers, any attempt to destroy or remove digital forensic evidence is also recorded as evidence against it (Ali Hassan Muhammad Al-Talaba, p199), and this is one of the most important advantages it enjoys compared to physical (traditional) evidence.

From this, it becomes clear to us that the French legislator has relied on this evidence, including digital forensic evidence, realizing the certainty of its results, but on the condition that it is subject to a set of conditions, the most important of which is that it is obtained in a legal and fair manner, and that it is discussed in the presence of all parties to the public lawsuit.

Second requirement: The position of Algerian legislation on digital forensic evidence

Before stating the position of the Algerian legislator on digital criminal evidence, The Algerian Code of Criminal Procedure, upon examination of its relevant articles, reveals a clear adoption of the free evidence system, mirroring the approach taken by the French legislator. This is evidenced by the enshrinement of the principle of the judge's *intime conviction* (personal conviction), a point underscored by Abdel Nasser Mohamed Mahmoud Farghali (2011, p. 15). Article 212 of the Code of Criminal Procedure explicitly states: "Crimes may be proven by any means of proof, except in cases where the law provides otherwise, and the judge may issue his judgment based on his own conviction..." This language closely mirrors the French approach, establishing a broad principle of admissibility while acknowledging the possibility of specific legal exceptions. The key phrase here is the judge's "own conviction," which signifies that the judge, after



.....

considering all admissible evidence, forms a personal, reasoned belief about the facts of the case.

Further reinforcing this interpretation, Article 307 of the same Code stipulates the same principle, stating: "...The law does not require judges to provide an account of the means by which they have reached their conviction." This provision underscores the subjective element of the judge's decision-making process. While the judge's conviction must be reasoned and based on the evidence, the law does not mandate a detailed explanation of the precise mental process by which that conviction was reached. This reflects the inherent limitations of articulating subjective belief and the trust placed in the judge's impartiality and judgment. Taken together, Articles 212 and 307 clearly establish that the Algerian legal system, like the French system, operates under a free evidence model, where a wide range of evidence is, in principle, admissible, and the judge's reasoned personal conviction plays a central role in the decision-making process. The absence of a requirement to explain the precise path to conviction further underscores the emphasis on the judge's subjective, yet reasoned, assessment of the totality of the evidence, nor does it set rules for them to which they must be subject, especially in assessing the completeness or sufficiency of a certain piece of evidence, but it orders them to ask themselves in silence and deliberation, and to sincerely search their consciences for any effect that the evidence attributed to the accused and the aspects of defending it have had on their perception. The law has only set this question for them, which includes the entire scope of their duties. Do you have Personal conviction?

It is noted that the text of Article 212 of the Code of Criminal Procedure includes an exception to the inadmissibility of proving some crimes by any means of proof. This means that the legislator in this case has adopted the restricted (legal) proof system as an exception in some crimes exclusively specified by law. An example of this is the crime of adultery stipulated in

Article 339 of the Penal Code, which Article 341 of the same law specified the evidence proving it exclusively (Ahmed Abdellah Hilali, p 722).

Therefore, by referring to the position of the Algerian legislator on digital forensic evidence, and based on the text of Article 212 of the Code of Criminal Procedure, in which the legislator permitted the proof of crimes by any means of proof, and through which he granted the judge the freedom to assess the evidence based on his personal conviction, it can be said that the legislator followed the French legislator by considering digital forensic evidence like other forensic evidence (Bouزيد Aghliss, 2019, p 110), and that the discretionary power enjoyed by the judge extends to include all forensic evidence, including digital evidence. Therefore, this type of evidence also does not raise a problem for the Algerian legislator as long as he embraces the freedom of proof, and the judge is only required to respect the general rules related to the acceptance of forensic evidence before the judiciary, which may take the form of reports following the inspection or interception of correspondence, for example, or also take the form of a technical expert report on the occasion of the inspection, examination and analysis of digital forensic evidence resulting from computers and their accessories (Article 341 of the Penal Code states that: "The evidence that is accepted regarding the commission of the crime punishable under Article 339 is based either on a judicial report prepared by a judicial police officer regarding a case of flagrante delicto, or on a confession contained in letters or documents issued by the accused, or on a judicial confession.").

Accordingly, if it is related to reports, the Algerian legislator considered them, as a general rule, to be mere inferences unless the law stipulates otherwise, which is what Article 215 of the Code of Criminal Procedure stated, stating: "The reports and reports proving felonies or misdemeanors shall be considered mere inferences unless the law stipulates otherwise." Article 214 of the same law also stated that: "The report or report shall have



no evidential force unless it is correct in form and has been prepared by its author during the performance of his duties and includes in it what he saw, heard, or witnessed himself on a subject within the scope of his jurisdiction.” However, the reports that the law authorizes judicial police officers to prepare by a special text to prove a specific misdemeanor(Naim Saeedani, 2013, p 229), these reports are considered authoritative unless they are refuted by evidence to the contrary, according to what is stipulated in Article 216 of the same law, which states: “In cases where the law authorizes by a special text judicial police officers or their assistants or employees and their assistants entrusted with some judicial control tasks the authority to prove misdemeanors in reports or reports, these reports or reports shall have their authoritativeness unless they are refuted by evidence to the contrary in writing or witness testimony.” As for technical expertise reports, the Algerian legislator considered them as well as other evidence of proof by subjecting them to the discretionary power of the judge, which was confirmed by the aforementioned Article 215, but the scientific and technical nature of cybercrime often requires the judge to rely on them in forming his personal conviction and to adhere to what the expert has reached, based on the fact that the judge cannot comprehend the scientific principles of digital forensic evidence despite his legal training (Khaled Ayad Al-Halabi, p 247).

Therefore, we arrive at the end and to clarify the judge's authority in assessing digital forensic evidence, we must distinguish between two matters, the first matter is the conclusive value of the evidence, and the second matter is the circumstances and conditions in which this evidence was found (Ahmed Abdel-ah Hilali, p724), and therefore the judge's assessment does not address the first matter, because the value of the evidence is based on precise scientific foundations, and the judge has no freedom to discuss established scientific facts, and as for the circumstances and conditions in which this evidence was found and surrounding it, they fall within the scope of his personal assessment.

Therefore, relying on digital forensic evidence and dealing with it by the criminal judicial bodies does not raise any legal problem as long as the Algerian and French legislations adopt the free evidence system, and on the other hand, it does not raise any technical problem due to the clarity of digital forensic evidence and its accuracy in proof.

In addition, it is possible to trace, extract and access its sources accurately, given that it is based on confirmed mathematical theories that are not tainted by any doubt, which strengthens its certainty in proof (Muhammad Al-Amin Al-Bishri, 1995, p 251).

Conclusion:

Digital forensic evidence is distinguished from other forensic evidence in that it is scientific evidence of a technical nature, through the fact that its extraction and analysis requires unconventional methods and techniques based on computer science and its laws, and it is also of a dual nature because the information and data extracted from computers or their networks are originally in digital form, in addition to that it is also diverse and advanced evidence, as it includes all information and data stored or processed by the computer or its accessories or even circulated on the Internet.

On the other hand, and in recognition of the importance of this type of evidence, the Algerian legislator has worked to create new procedural rules that are consistent with the specificity of cybercrime and its evidence, similar to what the French legislator has done, and based on the inability of traditional procedural rules in dealing with digital criminal evidence, based on the above, we conclude the following results and recommendations:

Results:

- It can be said that no matter how high the scientific and technical value of digital criminal evidence in proof, the judge must have discretionary power, because the latter is a crisis in order to make the scientific truth a judicial truth.



.....

- Digital criminal evidence presents unique challenges to the justice system, stemming from both the methods of its acquisition and its inherent nature. The process of obtaining digital evidence often necessitates complex technical and scientific operations, requiring specialized expertise and tools. Unlike traditional forms of evidence, digital evidence is often ephemeral and volatile. It can be easily altered, deleted, or overwritten, making it crucial to secure and preserve it quickly and effectively. Furthermore, the non-material nature of digital evidence creates a significant obstacle. Perpetrators of cybercrime can exploit this characteristic to their advantage, easily concealing, destroying, or encrypting digital evidence to prevent access by law enforcement. This inherent vulnerability poses a serious challenge to investigators and prosecutors, who must overcome these technical and logistical hurdles to effectively utilize digital evidence in criminal proceedings. The ease with which digital evidence can be manipulated or destroyed also raises concerns about its authenticity and integrity, requiring robust forensic procedures to ensure that the evidence presented in court is reliable and untainted. These combined difficulties—the complex technical operations required for acquisition and the volatile, non-material nature of the evidence itself—create a formidable challenge for law enforcement and the judiciary in the fight against cybercrime.

Recommendations:

- The need to legislate a special law for cybercrime similar to the Saudi Anti-Cybercrime Law and the UAE Anti-Information Technology Law, and to benefit from precedent laws.
- Strengthening international cooperation and exchanging knowledge and expertise with regional countries.
- Training and qualifying judges with technical and technological knowledge through specialized courses in modern technology.
- Including the subject of scientific evidence in curricula, whether in universities or in training institutes for judges and

lawyers, to remove the ambiguity surrounding this evidence and its validity in criminal proof.

List of sources and references:

- 1- Order No. 66-156 dated 06/08/1966, including the Penal Code, Official Journal No. 49, issued on 06/11/1966, as amended and supplemented.
- 2- Law No. 09-04 dated 08/16/2009, including the special rules for the prevention and combating of crimes related to information and communication technologies, Official Journal No. 47 of 2009.
- 3- Order No. 155-66 dated 06/08/1966, including the Code of Criminal Procedure, as amended and supplemented.
- 4- Abbas Al-Aboudi, Challenges of Proof by Electronic Documents and Requirements of the Legal System to Overcome Them, First Edition, Al-Halabi Legal Publications, Lebanon, 2010.
- 5- Muhammad Hussein Mansour, Evidence Law (Electronic Evidence), Dar Al-Jamia Al-Jadida for Publishing, Alexandria, 2004.
- 6- Khaled Ayyad Al-Halabi, Investigation and Investigation Procedures in Computer and Internet Crimes, First Edition, Dar Al-Thaqafa for Publishing and Distribution, Jordan, 1120.
- 7- Nasr Al-Din Marouk, Lectures in Criminal Evidence (General Theory of Criminal Evidence), Part One, Dar Houma, Algeria, 2003.
- 8- Kamal Muhammad Awad, Sharia and Legal Controls for Criminal Evidence (In Islamic Jurisprudence and Positive Law), First Edition, Dar Al-Fikr Al-Jami'i, Egypt, 2011.
- 9- Ahmed Abdel-Lah Hilali, "The Authenticity of Computer Outputs in Criminal Matters (Comparative Study)", in the Research of the Law, Computer and Internet Conference, Volume II, Edition Third, United Arab Emirates University, United Arab Emirates, 2004.



- 10- Ali Hassan Mohammed Al-Talaba, Criminal Inspection of Computer and Internet Systems (Comparative Study), First Edition, Modern World of Books, Jordan, 2004.
- 11- Moatasem Khamis Mshasha, "Proving Crime with Scientific Evidence", Sharia and Law Journal, Issue 56, United Arab Emirates University, United Arab Emirates, 2013.
- 12- Suzan Adnan Al-Ustadh, Violation of the Sanctity of Private Life via the Internet (Comparative Study), Damascus University Journal for Economic and Legal Sciences, Issue 3, Volume 29, Syria, 2013.
- 13- Abdul Nasser Mohammed Mahmoud Farghali and Mohammed Obaid Saif Saeed Al-Masmari, Criminal Evidence with Digital Evidence from the Legal and Technical Perspectives (Comparative Applied Study), Naif Arab University for Security Sciences, Saudi Arabia, 2011.
- 14- Bouzid Aghliss, the Principle of Free Evidence Correlates with the Self-Conviction of the Criminal Judge (A Comparative Analytical Study between Algerian Law, Egyptian Law and Some Arab Laws), Dar Al-Hoda, Algeria.
- 15- Naim Saeedani, Research and Investigation Mechanisms for Cybercrime in Algerian Law, Master's Thesis, University of Hadj Lakhdar Batna, Faculty of Law and Political Science, Algeria, 2013.
- 16- Mohamed El Amin El Bishri, Investigation of Emerging Crimes, Digital Forensic Evidence (Its Concept and Role in Proof)(, Arab Journal of Security Studies and Training, Issue 33, Volume 17, Naif Arab Academy for Security Sciences, Saudi Arabia, 5199.
- 17- Ali Ghribi, Digital Forensic Evidence - Concept and Authenticity -, a paper presented within the framework of the international conference on "Modern Criminal Evidence in Comparative Legislation" at the Faculty of Law and Political Science, University of Bechar on April 25/26, 2018.
- 18- Robin Widdson , Electronic Law Practice, An Exercise in legal futurology. Modern Law Review, Volume 66, Mach, 1997.

19-Peter Sommer, Peter Sommer, Digital Evidence, Digital Investigation and EDisclosure (A Guide to Forensic Readiness for Organizations, Security Advisers and Lawyers), Third Edition, Information Assurance Advisory Council (I.A.A.C), United Kingdom, 2011.