Contemporary Readings in Law and Social Justice
ISSN: 1948-9137, e-ISSN: 2162-2752
Vol 17 (01), 2025
pp. 812 - 825

The Impact of Digital Evidence Privacy on Cybercrime Prosecution

Abdelkader Amimer[1]*

[1]Faculty of Law, University of Algiers 1, Algeria. aek.amimer@hotmail.com

ABSTRACT: This study explores the impact of modern technology on the nature of cybercrime evidence, which is invisible and intangible. The study also examines the impact on the methods used in investigating and inquiring into this type of evidence, as well as the procedures for presenting it in court. Furthermore, the study addresses the handling of this new, notably complex and multifaceted type of evidence and the extent to which judicial discretion remains stable in the face of scientific evidence that is, in principle, free from ambiguity or doubt regarding its validity. We present the results derived from our findings on these points.

Keywords: digital evidence, cybercrime, judicial discretion, personal conviction of the criminal judge.

Received: 20/12/2024 **Accepted :01/08/2025** **Published: 17/09/2025**

Introduction

The emergence of cybercrime, which has characteristics that distinguish it from other types of crime, has also given rise to a new form of evidence that differs from traditional evidence. This is referred to as digital evidence and is characterised by features and specifications that require the handling of law enforcement, specialised scientific laboratories, judges and legal assistants, such as experts and attorneys, to possess unconventional skills and knowledge. This raises serious questions about the impact of these characteristics on the prosecution of cybercrime. In order to assess this impact, we sought to explore the nature of this evidence, its characteristics and its influence on judicial discretion.

Section One: The Nature of Digital Evidence

Digital evidence is a product of modern technology and is a reliable means of proving cybercrime has occurred. Digital evidence is a decisive indicator of cybercrime, particularly when experiments are accurately repeated by skilled experts. However, it often remains limited in its attribution to a specific individual. What, then, is the definition of this emerging type of evidence? What are its characteristics, and how does it compare to traditional criminal evidence in terms of its ability to prove cases?

Subsection One: Definition of Digital Evidence

This subsection will attempt to define digital evidence from both jurisprudential and legal perspectives.

Branch One: The Definition of Digital Evidence in Jurisprudence

In jurisprudence, digital evidence is defined as 'evidence obtained from computers in the form of fields, magnetic or electrical pulses, which can be collected and analysed using software applications and technology'. It is a digital component that presents information in various forms, such as written text, images, sounds, shapes, and graphics, for use by law enforcement agencies.

In the American report presented to the Interpol Scientific Symposium on Digital Evidence in 2001, it was defined as "data that can be prepared, transmitted and stored digitally, thereby enabling a computer to perform a specific task". It is also defined as 'evidence that exists in the virtual world in all its forms and manifestations'.

Digital evidence is referred to as 'digital' because the data in the virtual world, in all its forms — whether images, recordings or text — takes the form of binary numbers (0, 1), which are converted into images, recordings or text for display.

In summary, digital evidence can be described as logically and scientifically valid information obtained through legal and scientific procedures by translating computational data stored in computers, peripherals and communication networks. It can be used at any stage of an investigation or trial to prove a crime-related act, object, or person.

In the American report presented to the Interpol Scientific Symposium on Digital Evidence in 2001, it was defined as "data that can be prepared, transmitted and stored digitally, thereby enabling a computer to perform a specific task". It is also defined as 'evidence that exists in the virtual world in all its forms and manifestations'.

Digital evidence is referred to as 'digital' because the data in the virtual world, in all its forms — whether images, recordings or text — takes the form of binary numbers (0, 1), which are converted into images, recordings or text when displayed.

In summary, digital evidence can be described as logically and scientifically valid information obtained through legal and scientific procedures by translating computational data stored in computers, peripherals and communication networks. It can be used at any stage of an investigation or trial to prove a crime-related act, object, or person.

Digital evidence is similar to software in terms of its composition, the digital form it takes and its technical nature, which is based on the binary system of zeroes and ones. However, they are distinguished by the function or role they perform. While software operates the computer and directs it to solve problems and develop plans, without software, the computer is a useless machine. There are also types of software that assist in obtaining digital evidence, such as file processing and copying programs. In contrast, digital evidence is limited to proving cybercrime and attributing it to its perpetrators.

Branch Two: Legal Definition of Digital Evidence

Comparative legislation, including Algerian legislation, has not defined digital evidence as this is not the legislator's responsibility. This is a sensible approach, given that the unique characteristics of digital evidence could lead to negative practical implications if it were defined.

Furthermore, the Algerian legislator has not used this term in any legal texts related to this subject, including the Penal Code, Law 09-04 on specific rules for preventing and combating ICT-related crimes, and Decree 261-15 on the National Authority for Preventing ICT Crimes.

Subsection Two: Characteristics and Features of Digital Evidence

Due to the unique nature of cybercrimes, the evidence used to prove them differs from that used in traditional criminal cases. This type of evidence exists in an environment that is constantly evolving and contains various forms of digital data that can collectively or individually serve as evidence for conviction or acquittal. Therefore, digital evidence is regarded as the primary means of proving cybercrimes. It possesses several characteristics, outlined as follows:

Branch One: Digital evidence is intangible.

Some argue that digital evidence is intangible, meaning it lacks physical presence, unlike traditional evidence. However, translating and presenting it in a tangible form does not imply that this physical

compilation is the evidence itself. Rather, this process merely transfers those fields from their digital nature to a format that can be used to infer specific information. Conversely, others assert that the ability of digital evidence to be materialised enhances its validity and reliability, provided the scientific principles of the process and the conditions required for its execution are adhered to.

Branch Two: Digital Evidence as Technical Evidence

Digital evidence inherits its technical nature from the environment in which it exists, as well as from the machines and devices from which it is extracted, such as computers and other information systems. This characteristic has several implications, one being that access to this type of evidence is limited to specialists with the necessary technical knowledge and expertise. Additionally, this type of evidence can easily be erased. However, the perpetrator may sometimes lose control over this type of evidence due to its dynamic nature, enabling it to move from one location to another via communication networks. It can also provide one or more copies alongside the original, leading some legal scholars to describe it as evidence that is impervious to destruction, loss or alteration. The technical nature of digital evidence also necessitates special devices to collect and analyse its content, as well as specific software to ensure its integrity against manipulation and tampering.

Branch Three: Digital Evidence as Scientific Evidence

The elements that constitute digital evidence — namely, data and information — are inherently intangible, whether loaded, stored or transmitted in digital form. Therefore, to perceive and obtain this type of evidence, electronic devices and equipment of the same nature must be utilised, along with specific programmes and systems. This implies that, as evidence, it requires a technical environment in which it is formed, given its information technology-related nature. Consequently, the principles applicable to scientific evidence generally also apply to digital evidence. This type of evidence should therefore not deviate from what has been established by digital science; otherwise, it loses its meaning.

Branch Four: Digital Evidence as Advanced Evidence

Digital evidence is advanced evidence. It is characterised by a highly dynamic nature that enables it to move from one location to another through communication networks, unaffected by the limitations of time and space.

Digital evidence is characterised by its highly dynamic nature, which enables it to move through communication networks, unaffected by the limitations of time and space. Unlike traditional evidence, which must be present at the crime scene, directly connected to it, or result from it, these attributes do not fully apply to digital evidence. This type of evidence can be obtained from a location far removed from the crime scene or the realisation of its outcome. Its connection to a virtual scene enables retrieval from distant places within the digital space by individuals or entities not connected to the crime, such as internet service providers, who may possess knowledge of certain cybercrime-related details.

Branch Five: Digital Evidence is Recoverable

One characteristic of digital evidence is that it can be recovered after deletion. Deleted files often remain in a recoverable state for a long time, as the digital footprint cannot be completely erased. There are numerous software programs designed for this purpose, which only require some level of expertise to use. Recovered evidence has the same scientific value and probative force as original evidence — a feature not found in traditional evidence. This characteristic provides strong protection against the loss, destruction or alteration of digital evidence.

Section Two: The Impact of the Unique Nature of Digital Evidence on the Criminal Judge's Discretion

Our previous study concluded that digital evidence has characteristics and features that distinguish it from other types of evidence. Does this affect the judge's discretion?

Subsection One: The Concept of Judicial Discretion in Criminal Law and Its Manifestations

Legal scholars and courts have established that criminal judges possess broad discretionary authority when evaluating evidence and inferring implications from the facts. This view naturally extends to digital evidence, since the assessment of evidence in criminal matters is based on the idea that evidence neither creates nor confirms the truth, but is merely one aspect of it. Judicial truth is considered relative, not absolute. For example, evidence presented for discussion may include a forged document or false testimony, or a confession may be given with the intention of misleading and concealing the truth. The same applies to digital evidence, which can be subject to manipulation and tampering through modifications that distort the truth. This justifies granting the judge the freedom to assess the validity of the evidence presented to them, accepting it if they are convinced of its authenticity and disregarding it if they harbour doubts about its validity.

Branch One: The Concept of Judicial Discretion in Criminal Law

The concept of judicial discretion is broad and has been the subject of numerous studies. The term 'discretion' refers to the authority to issue judgements and take the initiative. Some legal scholars define discretionary authority as 'the freedom of choice granted to an authority in exercising its competencies, allowing it to make a specific decision, refrain from taking action, or settle matters in a particular manner, determining the timing of intervention independently'. This definition pertains to discretionary authority in general, without specifying the authority or body to which it is granted. Described as discretionary, it refers to 'the pure will of the judge in assessing, weighing and measuring matters using logical criteria derived from their personal understanding of the objective facts and the appropriateness of these facts to the intended legal rule'. Thus, judicial action is a manifestation of authority and sovereignty, while legal action is a manifestation of the judge's freedom.

Judicial discretion has been defined as 'the mental and intellectual activity performed by the judge in understanding the reality presented to them and inferring the elements that bring this reality within the scope of a specific legal rule'. By exercising his discretionary authority, the judge performs two main tasks: examining the facts and applying the relevant law.

Branch Two: Manifestations of Judicial Discretion in Criminal Law

The manifestations of judicial discretion can be summarised as follows:

First: The judge's authority to exclude evidence

Under the system of personal conviction, the criminal judge has the authority to accept all evidence, and it cannot be argued that there is any evidence from which he may not derive his conviction. The judge has complete freedom to select the evidence that forms their personal conviction, and this may include any presumption or proof as the basis for their ruling. Under this system, the judge has the authority to weigh and assess evidence in order to reveal the truth, provided it is clear and free from ambiguity or doubt, regardless of its source, so long as it is lawful. Consequently, he has the authority to exclude any evidence that he finds unconvincing or that does not convince him. This also applies to digital evidence: if the judge is not convinced by it, they can exclude it and rely on another piece of evidence instead.

Secondly, the judge has the authority to fragment evidence or accept it in full.

In the context of personal conviction, the judge may accept the evidence in its entirety, or fragment it and accept what he deems appropriate while excluding the rest. For instance, he may accept part of a defendant's confession while disregarding another part, or accept the same evidence for one defendant while rejecting it for another. The same principle applies to digital evidence: the judge may accept part of it and reject the rest, or accept it in full.

Thirdly, the judge's authority to assess evidence collectively.

The judge may form their own personal opinion based on the evidence as a whole, a principle known as the interdependence of evidence. This means that all the evidence presented in a case supports each other, forming a cohesive structure. Any flaw in this structure could cause the whole case to collapse. This principle applies to digital evidence when it is presented alongside other evidence in the case file, regardless of the nature of the evidence.

Fourth: The judge's authority to search for truth wherever it may be found.

This is referred to as the positive role of the judge and implies that they are not limited to the evidence presented by the parties involved in the case. They have the authority to take the initiative and undertake all necessary actions to investigate the case and uncover the truth. The truth does not reveal itself spontaneously; it always requires someone to search for and excavate it. If the judge is not convinced by the evidence presented by the parties, the law empowers him to seek the necessary evidence to reach a correct conviction and reveal the truth in all its aspects.

One manifestation of the judge's positive role in seeking evidence in cybercrime is his authority to direct service providers to grant him access to data allowing him to identify the websites visited by the defendant, as well as the sender and recipient. Furthermore, he can enlist system operators to provide the necessary information to access and search the information system and locate evidence.

Subsection Two: The Judge's Personal Conviction as the Basis for Assessing Digital Evidence

The empowerment of investigative authorities with modern and advanced scientific tools for the purpose of investigating cybercrime, along with the potential errors that may affect individuals' rights and freedoms, has made it necessary to subject the resulting evidence to the authority of the judge. This ensures the protection of individuals' rights and freedoms against the consequences of such errors. This has led me to dedicate the first branch of this subsection to the concept of this principle and the second branch to the extent to which the unique nature of digital evidence affects the judicial discretion of the criminal judge.

Branch One: Definition of the Judge's Personal Conviction

In legal systems, the term 'personal conviction' often refers to a system of moral or emotional proof. This implies that judges are granted broad discretion to assess the value of the evidence presented in a case. This issue arises when the judge is presented with evidence supporting the defendant's involvement in the criminal act, alongside evidence refuting the charges against them. This gives the judge full authority to weigh one against the other.

Some legal scholars argue that the judge's personal conviction is a psychological tendency aimed at applying the law. This has been defined as 'a firm impression that arises in the judge as a result of a scientific, mental and logical process that stirs in the judge's mind and conscience, influenced by the facts presented to them and their perceptions and models of truth'. Ultimately, this process leads to either a strong acceptance and firm belief that reassures the judge's conscience and heart, leaving no room for doubt regarding the defendant's guilt; doubt regarding the defendant's guilt, leading the judge to acquit; or an impression pertaining to jurisdiction over the case or its admissibility, allowing the judge to rule without addressing the merits. It has also been defined as 'the discretionary assessment of the elements of proof in the case, serving as an alternative to the system of legal evidence'.

From the previous discussion, we conclude that, in a system embracing the concept of the judge's personal conviction, the judge has considerable freedom when evaluating proof, weighing evidence and making assessments. It is through the formation of his conviction in the case before him that the characteristics of his discretionary authority emerge. Under this system, the judge can base his ruling on any evidence or presumption that he deems relevant, without being subject to oversight by the Supreme Court, which cannot question his conviction. However, he must consider sound logic and the exceptions imposed by law; otherwise, his ruling may be annulled.

Branch Two: The Admissibility of Digital Evidence

The admissibility of evidence in criminal proceedings relates to the ability of the evidence to persuade the judge. Admissibility is measured by two factors: the first is subjective, referring to admissibility in the narrow sense, i.e. the persuasive power of the evidence; the second is relative, referring to the ability of the evidence to stand up against other evidence. Opinions among legal scholars regarding the admissibility of digital evidence vary. Some grant digital evidence absolute admissibility, which nullifies the judge's authority to assess it. Others consider digital evidence to have relative admissibility due to the possibility of manipulation and distortion. We will examine these two viewpoints below.

First: The absolute admissibility of digital evidence in proof.

The admissibility of digital evidence is a topic of debate among legal scholars. Some argue that this type of evidence should be removed from the criminal judge's discretionary authority. It has been suggested that, given that it fulfils the conditions of certainty, digital evidence should have binding authority for the judge. In theory, this would make it unacceptable for the judge to exercise their authority to verify the facts expressed by the evidence.

Proponents of this view also argue that the accuracy and objectivity of digital evidence, along with its unique nature, threaten the principle of the judge forming their own personal conviction. The purely scientific nature of this evidence can render the judge unable to challenge it as a means of proof, thereby reducing their discretionary authority. This directly impacts the formation of the judge's personal conviction, potentially leading to its rejection in some cases. If the digital evidence does not align with the judge's established personal conviction, he may find himself in a dilemma, with two options: to abandon his personal conviction and accept the digital evidence, or to exclude it from consideration.

Second: the relative admissibility of digital evidence as proof.

Those who oppose the previous view of the absolute admissibility of digital evidence argue that merely obtaining and presenting it to the court is insufficient for it to be relied upon in a conviction. This is due to the technical nature of this evidence, which allows its content to be manipulated in ways that can distort the truth, often beyond the perception of non-specialists. Furthermore, errors in the procedures for obtaining credible evidence that accurately reflects the truth appear to be common in this type of evidence.

Consequently, doubts arise regarding the credibility of digital evidence as proof in criminal proceedings. This concern relates not to the content of the digital evidence itself, but to independent factors affecting its credibility. Therefore, it is essential to verify the integrity of the digital evidence with regard to any defects, and to subject it to technical evaluation, in order to avoid flaws that may affect its reliability. This can be achieved using technical methods appropriate to this type of evidence, enabling examination to ensure its integrity and the correctness of the procedures used to obtain it.

Moreover, digital evidence does not replace traditional methods of proof; it is often used to prove that a crime occurred rather than to attribute it to the defendant or exonerate them. Consequently, digital evidence has a more evident impact on the judge's personal conviction when establishing the occurrence of a crime than when attributing or disproving facts to the defendant.

Legal scholars have differing opinions on the value of judicial expertise in general, including technical expertise, in cases related to cybercrimes. They are divided into three perspectives:

First Perspective:

Proponents of this view argue that the criminal judge must adhere to the findings reached by the expert in their report. This perspective is championed by scholar Enrico Ferri, a pioneer of the positivist school, who stated in his book on sociology: "We demand that expertise be binding on the judge because the expert is more competent than he is in a purely technical subject." Similarly, scholar Garofalo criticized the principle that "the judge is the supreme expert" or "the judge is the expert of experts." He argued that, practically

speaking, the expert's opinion directs the judge in forming his conviction. He believes it is challenging to accept the idea that a judge may disregard an expert report, especially when it addresses matters outside the judge's expertise. The expert's specialization and familiarity with the subject mean that assessing the report and overseeing its content do not fall within the judge's authority. Therefore, while the judge theoretically possesses absolute discretionary authority, he is practically bound by the expert reports. Ferri also contends that the principle of the judge being the expert of experts can only be realized if judges are trained adequately to verify the technical expertise and evaluations presented.

Second perspective: Advocates of this view believe that the judge is the ultimate expert and that expert opinions do not constrain him. They argue that the judge has absolute authority and complete freedom to assess the evidence presented to them, including expertise related to digital evidence. The judge is legally authorised to resolve the dispute before them and issue a ruling. In contrast, the expert's role is limited to providing a technical opinion on a matter related to the dispute brought before the judge. This highlights that the expert's opinion is not a judgement, but an advisory opinion that the judge is not obliged to follow. The judge alone has the authority to accept or reject the evidence presented, provided he justifies his decision. The judge's oversight of the expert involves a legal review of the technical opinion, resulting in a decision to either accept or exclude it.

However, the authority granted to the judge is subject to constraints and regulations that assist him in performing his duties and protect him from deviation and abuse. Among the regulations established by legal scholars for this purpose, which the judge should consider when reviewing the expert testimony, are the following questions: Were the laws and principles governing expert testimony meticulously observed, and were their provisions applied correctly? Were the expert's conclusions, summaries, and the supporting arguments sufficiently justified and reasoned? Is there consistency between the expert reports and the testimonies of witnesses or the confessions of the defendant? If there are multiple experts, is there a consensus among them?

Third perspective: Proponents of this view attempt to reconcile the previous two opinions by highlighting two key issues. The first relates to the definitive scientific value of the evidence itself, while the second concerns the circumstances in which it was found. According to this perspective, the judge should refrain from addressing the first issue — the definitive scientific value of the evidence — since this matter is beyond his area of expertise. This is why he seeks the assistance of an expert in this field. However, the judge can address the second issue by discussing the circumstances and context in which the evidence was found, since these fall within his discretionary authority. Despite its scientific certainty, he may disregard such evidence if he deems it to be logically inconsistent with the circumstances of the incident and its context.

Branch Three: The Scope of the Judge's Discretionary Authority Regarding Digital Evidence

Like other types of evidence, digital evidence is primarily subject to the judge's assessment, which is influenced by his personal conviction. However, the judge's assessment does not include the definitive scientific value of the evidence, taking into account its scientific nature, objectivity, neutrality and reliability. Instead, the judge may consider the circumstances and context in which the digital evidence was found.

First: The Definitive Scientific Value of Digital Evidence

The scientific value of digital evidence is an issue that falls outside the judge's knowledge and expertise, as it is based on precise scientific foundations. Discussing established scientific facts does not fall within the judge's responsibilities but rather pertains to specialists and experts, a role that the court cannot replace. This leads to the conclusion that digital evidence is merely an application of scientific evidence characterized by objectivity, neutrality, and competence in persuading the judge. The judge's role is limited to assessing whether the legal conditions for its admissibility are met; if they are, he accepts it, and if not, he excludes it from the acceptable evidence.

Concerns may arise regarding the integrity of digital evidence, particularly with regard to its susceptibility to manipulation. For example, evidence that was created to prove one fact could be presented as proof for another, unrelated fact, which may go unnoticed by an ordinary person. A second concern could be errors when using the correct tools to obtain evidence or incorrect specifications. Thus, doubts about digital evidence stem not from its content, but from external factors affecting its admissibility. This necessitates the use of technical means appropriate to this type of evidence in order to examine and ensure its integrity, as well as the correctness of the procedures followed in obtaining it.

In summary, regardless of its precision, scientific evidence is always subject to the judge's discretionary authority, which monitors for fraud or error and excludes evidence if such issues are present. This is also essential for transforming scientific truth into judicial truth.

1. Evaluating digital evidence regarding the technical integrity of the procedures used to obtain it:

The technical procedures used to obtain digital evidence may contain errors that call the validity of the results into question. To ensure the integrity of these procedures, several methods can be employed, including the 'Dauport' tests. These tests verify the soundness of the procedures used to obtain the digital evidence and ensure that it can be accepted as proof. Steps taken to ensure the technical integrity of these procedures involve subjecting the tools used to various tests to confirm their accuracy in yielding the desired results. Two main tests are followed:

False Negatives Test: The purpose of this test is to subject the tool used to obtain the evidence to an examination that demonstrates its ability to present all relevant data related to the digital evidence, ensuring that no important information is overlooked.

False Positives Test: This involves subjecting the tool used to obtain the digital evidence to a technical test that verifies the tool does not present any new additional data. Through these two tests, it can be confirmed that the tool used has displayed all data related to the digital evidence while simultaneously not adding any new information. This lends credibility to the results provided by that tool in demonstrating reality.

Additionally, one can rely on tools proven effective in scientific research to achieve better results. Published research in the field of information technology indicates the proper methods for obtaining digital evidence and highlights tools whose efficacy is questionable. This helps to determine the credibility of outcomes derived from these tools.

2. Evaluating digital evidence regarding its integrity against tampering

Ensuring the integrity of digital evidence against tampering is one of the most critical criteria for proving its credibility. This criterion confirms that the digital data collected matches the original data. Computers play a significant role in providing the technical information that contributes to our understanding of the content and form of digital evidence. Therefore, it is essential to preserve the evidence and provide a means of tracing the steps used in its collection and the results obtained.

The integrity criterion verifies whether any changes have been made to the digital evidence and whether it remains consistent with the original content during the collection process. There are several ways to ensure the integrity of digital evidence against tampering, including analogue analysis, in which computer science plays an important role in providing technical information that aids understanding of the content and form of the digital evidence. These sciences help to reveal the extent to which the contents of this evidence have been tampered with.

The concept of digital analog analysis is one of the important means for verifying the credibility of digital evidence. Through this method, the digital evidence presented to the court is compared with the original data recorded in the automated data processing system. This allows for confirming whether any tampering has occurred in the extracted version. Additionally, algorithms can be utilized if the original version of the digital evidence is unavailable or if tampering has occurred with the original version. In such cases, the

integrity of the digital evidence can be confirmed against alteration or tampering through the use of specific computational operations known as algorithms.

Another method that can be used to evaluate the integrity of digital evidence against tampering is called neutral evidence. This evidence is unrelated to the crime itself, but it can be used to verify the integrity of the digital evidence in question, i.e. whether any modification or change has occurred in the automated data processing system.

It can therefore be concluded that doubts about the integrity of digital evidence due to its susceptibility to tampering and errors in obtaining it are technical issues that judges cannot rule on definitively; this is a matter for specialists. If specialists confirm that the digital evidence meets the aforementioned conditions regarding its integrity and the acquisition process, then the judge cannot reject this evidence based on discretionary authority. For the judge to reject evidence based on doubt, there must be sufficient grounds to question the evidence. However, the judge cannot definitively assert this if the evidence meets the integrity conditions. The judge's role is limited to examining the evidence's connection to the crime, as assessing its credibility is primarily the expert's responsibility, not the judge's. In this case, the judge can only accept the evidence and cannot question its evidentiary value as it inherently represents a truthful account of reality, unless it is proven that there is no connection between the evidence and the intended crime.

However, there is a legal opinion that asserts that despite the accuracy of the results that can be reached through technical expertise regarding the integrity of digital evidence against tampering and the methods of obtaining it, such results are not sufficient by themselves as the sole evidence for proving cybercrime. This is because they are not independent scientific evidence; rather, they involve the exploration of indications followed by analysis and the extraction of their implications. Thus, they are not independent of the circumstantial evidence, which is one of the methods of proof.

However, a legal opinion asserts that, despite the accuracy of the results that can be obtained through technical expertise regarding the integrity of digital evidence and methods of obtaining it, such results alone are not sufficient to prove cybercrime. This is because they are not independent scientific evidence; rather, they involve exploring indications, followed by analysis and extracting their implications. Therefore, they are not independent of circumstantial evidence, which is one of the methods of proof.

This opinion has faced criticism, as considering scientific evidence resulting from technical expertise as merely circumstantial evidence that cannot be relied upon for conviction alone will allow cybercriminals to escape accountability and punishment. Proponents of this view advocate a departure from the current rule regarding the proof of cybercrime, arguing for reliance on scientific evidence derived from technical expertise as standalone proof. This is particularly pertinent given the absence of any legal text prohibiting it.

Secondly, we will discuss the circumstances and context in which the evidence was found.

The presence of digital evidence in a case before a criminal judge does not mean that they are obliged to rule based solely on it. Instead, the evidence is examined in light of the circumstances and context in which it was found. If the evidence conflicts with the circumstances of the incident, it may generate suspicion and doubt, not about its validity, but about its applicability to the facts and attribution to the defendant. In such cases, the judge applies the principle that doubt is resolved in favour of the defendant and excludes this evidence. Therefore, the circumstances and context in which the evidence was found are matters of the judge's discretionary authority, governed by the principle of equality of evidence. This qualifies the judge to exclude any digital evidence that does not align with the circumstances of the incident.

Conclusion:

Despite the uniqueness of digital evidence compared to traditional criminal evidence, which criminal evidence systems are not accustomed to, it still remains within the realm of the general theory of criminal proof. It is not possible to assert the existence of a specific evidentiary system that establishes special rules

for how digital evidence is handled by criminal judges outside the recognised general principles of proof. Nevertheless, the evidentiary strength of digital evidence has sparked various legal opinions concerning the diminishing principle of freedom of proof and the judge's personal conviction in the context of proving cybercrime. This gradual shift towards a more constrained evidentiary system is likely to lead to future discussions and proposals that will highlight the importance of this topic and shed more light on it.

References:

[1] Ahmed Youssef El-Tahawy, 'Electronic Evidence and its Role in Criminal Proof': A Comparative Study', Dar Al-Nahda Al-Arabiya, Cairo, Egypt, 2015.

[2] Mamdouh Abdel Hamid Abdel-Mottaleb, Digital Criminal Investigation and Research in Computer and Internet Crimes, Dar Al-Kutub Al-Qanuniyya, Egypt, 2006.

[3] Mohammad Amin Al-Bishri, Investigating Modern Crimes, Naif Arab University for Security Sciences, Riyadh, Saudi Arabia, 2004.

[4] Aisha bin Qara Mustafa, The Evidentiary Value of Evidence in the Field of Criminal Proof in Algerian Law and Comparative Law, Dar Al-Jami'a Al-Jadida, Egypt, 2010.

[5] Sharma, M., & Sharma, S. R. (2025). Advanced hydrological simulation and hybrid CNN-LSTM models for sustainable water resource management in Nepal. Journal of Information Systems Engineering and Management, 10(31s). https://doi.org/10.52783/jisem.v10i31s.5059

[6] Tariq Muhammad Al-Jamali, 'Digital Evidence in the Field of Criminal Proof', a working paper presented at the First Maghreb Conference on Informatics, Academy of Graduate Studies, Tripoli, Libya, 2009.

[7] Tarik Afifi Sadiq Ahmed, Electronic Crimes (Mobile Phone Crimes), The National Center for Legal Publications, Egypt, 2015.

[8] Khaled Ayad Al-Halabi, Investigation and Inquiry Procedures in Computer and Internet Crimes, Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2011.

[9] Omar Mohammad bin Younes, The Information Society and Electronic Government, Encyclopedia of Arab Legislation, 2003.

[10] Abdul Majeed Ibrahim Salim, 'The Discretionary Authority of the Legislator: A Comparative Study', Dar Al-Jami'a Al-Jadida, Alexandria, Egypt, 2010.

[11] Nabil Ismail Omar, The Discretionary Authority of the Judge in Civil Matters, Mansha'at Al-Ma'arif, Alexandria, 1st edition, 1984.

[12] K. Abdul Wahid Al-Johari, Regulations of the Criminal Judge's Freedom in Forming His Conviction and Fair Criminal Trial, The National Center for Legal Publications, Cairo, Egypt, 2015.

[13] Mahmoud Mahmoud Mustafa, Proof in Criminal Matters in Comparative Law, Cairo University Press, Egypt, 1977. 13.

[14] Ghazi Mubarak Al-Dhunibat, Technical Expertise in Proving Forgery in Handwritten Documents: Art and Law', Dar Al-Thaqafa for Publishing and Distribution, Amman, Jordan, 2005.

[15] Abdul Hamid Al-Shawarby, Criminal Proof in Light of the Judiciary and Jurisprudence, Mansha'at Al-Ma'arif, Alexandria, Egypt, no date.

[16] Hilali, Abd Al-Lah Ahmed, The Authority of Computer Outputs, Previous Reference, p. 103.

[17] Muhammad Hamdan Ashour, Methods of Investigation and Criminal Research, Palestine Academy for Security Sciences, Palestine, 2010.

[18] Ashraf Abdul Qadir Qandil, Criminal Proof in Electronic Crime, Dar Al-Jami'a Al-Jadida, Alexandria, Egypt, 2015.

[19] Lina Mohammad Al-Asadi, The Extent of the Effectiveness of the Provisions of Criminal Law in Combating Cybercrime: A Comparative Study, Dar Al-Hamid for Publishing and Distribution, Amman, Jordan, 2015.

[20] Abdul-Fattah Bayumi Hijazi, The Legal System for the Protection of Electronic Government, Dar Al-Matbuat Al-Jami'iya, Alexandria, Egypt, 2003. 20.

[21] Mohammad Hammad Murhej Al-Hiti, Cybercrime: Models of its Application (A Comparative Study), Dar Shatat for Publishing and Software, United Arab Emirates, 2014.

Theses and Dissertations:

1. Idris Lakrini. "Discretionary Authority of the Criminal Judge". PhD Thesis in Private Law, Faculty of Law, Fes, Morocco, Academic Year 2020/2001.

2. Hilali Abdel-Lah Ahmed. "General Theory of Evidence (Comparative Study)". PhD Thesis, Cairo University, Faculty of Law, Academic Year 1984/1985.

Articles and Papers:

1. Mamdouh Abdel-Hamid Abd Al-Muttalib, Zobaida Mohammad Qasim, Abdullah Abdul-Aziz. "Proposed Model for Rules of Acceptance of Digital Evidence in Computer Crimes". Paper presented at the Conference on Banking and Electronic Transactions, Faculty of Sharia and Law, United Arab Emirates University, held from May 10-12, 2003, Vol. 5.

Foreign References:

1. GARRAUD (R). Traité théorique et pratique d'instruction criminelle et de procédure. Vol. V. Paris: Sirey, 1929.