



The Legitimacy of Electronic Evidence in Criminal Proceedings

Abdelkader Amri *

College of Law - University Yahia
Fares - Medea (Algeria)

Avocat.amri@yahoo.fr

Benferhat Noureddine

College of Law - University Yahia Fares -
Medea (Algeria)

benferhat.noureddine@univ-medea.dz

Abstract

The criminal and electronic evidence are deemed essential in investigation and trial proceedings, serving as means to ascertain the truth. Electronic evidence is characterized by precision and difficulty in tampering with, necessitating adherence to laws and procedures to ensure its legitimacy. It must be reliable and compliant with legal and ethical standards, with the judge relying on digital evidence to make decisions and transparently discussing them in the courtroom to achieve justice and uphold the law accurately.

Article info

Received
February 20, 2024
Accepted
September 07, 2024

Keyword:

- ✓ Electronic evidence
- ✓ Investigation
- ✓ The legality

* Corresponding author

1. **Introduction**

Since half a century ago, the world has witnessed a radical transformation with the emergence of what is known as the Information Revolution, where information has become as essential as oil or energy in shaping the course of civilization. This revolution is linked to the advancement of technology and communications sector, especially with the widespread use of the Internet, which has become a fundamental means of exchanging information among individuals, entities, and nations.

At present, we find that countries and institutions heavily rely on information exchange in performing their daily operations. Information is now stored, processed, and transferred among various entities, whether within the country or across national borders, enabling the exchange of knowledge and fostering collaboration between nations.

However, this technological advancement has not come without challenges, as the emergence of electronic crimes and illegal data exploitation poses a serious threat to cybersecurity, personal privacy, and institutional security. With the rapid development of these crimes and the cunningness of their perpetrators, the justice system faces challenges in collecting evidence, proving crimes, and enforcing legal accountability. Therefore, understanding the importance and impact of the Information Revolution on economic, political, and social aspects contributes to the development of effective

strategies to address the new security challenges that arise with it.

Technology has evolved tremendously in recent decades, and despite the great benefits it has brought, it has also opened the door to new phenomena of crime and violations. Technological advancement has led to the emergence of electronic crimes, which is evident in the ease of their commission, execution, and the difficulty of their detection and prosecution.

The danger of these crimes lies in the ease with which they can be committed and their traces concealed. Perpetrators of electronic crimes often use the internet to store and exchange their data without detection, making it difficult for justice systems to track them and achieve justice. Additionally, their use of encryption and secret codes makes it extremely challenging to decipher the codes of their criminal activities.

This challenge puts significant pressure on the judicial and criminal investigation systems, requiring technical and technological skills to uncover these crimes, along with complex investigation procedures to identify and collect evidence legally. The trial of electronic crimes requires a different approach due to their unique nature and the challenges facing investigation and evidence processes. The methods of collecting and presenting evidence in these cases differ from the traditional methods used in prosecuting ordinary crimes. Electronic crimes require the use of special tools and techniques to detect and prove them in court.

The term "electronic evidence" refers to evidence related to electronic activities such as email, text messages, digital records, and so on. These pieces of evidence have technical and scientific characteristics that make them different from traditional evidence. Certain conditions must be met for electronic evidence to be admissible in court, including its credibility and integrity.

The role of electronic evidence in proving cases before the court and how it is used to present facts to the criminal justice system should be clarified. This evidence plays a vital role in proving electronic crimes and achieving justice, so understanding its characteristics and methods of collection and proper use before the court is crucial.

Through the foregoing, we raise the following issue: What is the validity of electronic evidence as a means of criminal proof?

To address this issue, we have opted for a descriptive-analytical approach by delving into a study and description of this electronic evidence, defining it, identifying the procedural and technical methods employed in obtaining it, affirming its legitimacy, and then examining its admissibility before the criminal judging.

2. The Concept of Electronic Evidence

2.1 Definition of Electronic Evidence

Definition of criminal evidence generally involves a means used by the judge to access the truth sought in the case, while electronic evidence is defined as evidence obtained from computers and other

electronic devices, which can be collected and analyzed using information processing techniques. The credibility of electronic evidence relies on the reliability and integrity of the data extracted from electronic devices and transmitted digitally. The importance of electronic evidence lies in its role in identifying electronic crimes and presenting them to justice correctly and effectively. Beginning with a general definition of criminal evidence, we will then define electronic evidence.

Definition of Criminal Evidence:

There are multiple definitions of criminal evidence, including:

Criminal evidence is defined as "the means by which the judge resorts to reach the truth sought after." The term "truth" here refers to all the details and events presented to the judge for him to make his legal decision based on them. (Ahmed Fathy Sorour (2010), *The Intermediary in Criminal Procedures Law*, Dar Al-Nahda Al-Arabiya, Cairo, p418). Other definitions consider criminal evidence as "the incident from which the judge derives evidence to prove his conviction of the judgment reached." (Mamoun Salama (2012), *Criminal Procedures in Egyptian Legislation*, Dar Al-Nahda Al-Arabiya, Cairo, p191.)

Some have defined it as "the legitimate probative means that contribute to achieving a state of certainty in the mind of the judge in a permissible manner, ensuring satisfaction and leading the mind to the judgments imposed on it."

This sentence indicates that evidence in criminal cases differs from evidence in other laws, (Abdel-Hafiz Abdel-Hadi Aabid, Criminal Proof by Indications, Ph.D. thesis, Faculty of Law, Cairo University, Egypt, 1989, p198.)

where criminal evidence is considered more stringent and more specific compared to evidence in other laws. The difference lies in the precision and strictness in the process of verifying facts and evaluating evidence in criminal matters, where there must be a high degree of judicial certainty before issuing any judgment.

Definition of Electronic Evidence:

Definitions related to electronic evidence have been diverse and varied, attributable to the specialization to which this evidence belongs, resulting in discrepancies between researchers in the technical and legal fields. Some legal scholars have defined electronic evidence as evidence obtained from computers, which may be in the form of fields, magnetic pulses, or electrical signals that can be collected and analyzed using specialized software, applications, and technology. It consists of digital content that presents information in various formats such as written texts, images, sounds, shapes, and drawings, for reliance and application before law enforcement agencies. (Mohammed Taqa Faleh Rashdan Al-Hawani, Validity of Electronic Evidence as a Means of Proof in Criminal Matters (A Comparative Study between Kuwaiti and Jordanian Laws), Master's thesis, Faculty of Law, Department of Public Law, University of the Middle East, Jordan, 2015, p 19-20.)

However, this definition appears to limit the concept of electronic evidence to those obtained from computers, restricting the scope of electronic evidence derived from any other electronic device. Electronic evidence plays a crucial role in the field of digital law, offering various and diverse definitions. A perspective of jurisprudence indicates that electronic evidence relies on information processing techniques and is utilized to convince the judge of the commission of a crime over the internet (Diaa Ali Ahmed Naaman (2011), Apparent Information Fraud and Applications: Legal Studies Series in the Field of Printed and National Paper Information, Morocco, p282.)

In this context, the International Organization for Computer Evidence (IOCE) defines electronic evidence as information bearing legal value that is stored or transmitted digitally Salama Mohammed Al-Mansouri, Application of the Principle of Spatial Conviction on Electronic Evidence, thesis submitted to fulfill the requirements for obtaining a Master's degree, Faculty of Law, Department of Public Law, United Arab Emirates University, United Arab Emirates, 2018, p18.)

Generally, electronic evidence assists in identifying the occurrence of cybercrimes, proving them, identifying perpetrators, prosecuting them, and implementing necessary penalties.

After reviewing the various definitions of electronic evidence, we notice a significant convergence among them. All of them attempt to accommodate this new type of

evidence, despite its association with the virtual world. However, there are some important observations to consider in this regard.

Some definitions have linked the concept of software with that of electronic evidence. Electronic evidence has been described as any information prepared or stored digitally, as if it were loaded onto a specific medium that can be read by a machine. This definition aligns with the concept of informational software.

Despite the similarity in their digital composition, the primary difference between electronic evidence and computer software lies in the function each performs. Computer software operates to execute various processes within the automated processing system, facilitated by a set of programs that enable it to carry out these operations when appropriate commands are given.

Electronic Evidence Divisions:

The U.S. Department of Justice classifies electronic evidence into three main categories as follows: (Najib Hind (2017), Validity of Electronic Evidence in Criminal Proof, National Criminal Journal, Egypt. Volume 60, Issue 2, p161-162.)

Records Stored in the Computer: This category includes written documents stored in the computer such as email, word processing files, and online chat messages.

Records Created by the Computer: This category includes records created by computer programs and not directly

touched by humans, such as log files, phone records, and ATM transaction receipts.

Records Containing Input and Output Data from the Computer: This category includes documents containing input data fed into programs like Excel and processed through the program by performing arithmetic operations.

Regardless of the access method, evidence remains digital. In all cases, digital evidence must be based on a virtual nature, even in the absence of digital capabilities in courts.

2.2 Characteristics of Electronic Evidence

In today's tech-driven world, electronic evidence plays a crucial role in legal proceedings and criminal investigations. It stands out for its scientific approach to uncovering truth through digital evidence and knowledge, as well as its agility and resilience against disposal attempts. Despite challenges in its admissibility, grasping these unique traits is essential for upholding justice and legal integrity in the digital era.

Electronic evidence operates within an advanced digital environment, encompassing various types of digital data that can be used individually or collectively to form a basis for conviction or exoneration. Electronic evidence possesses several distinct characteristics compared to traditional criminal evidence, the most significant of which are:

Scientific Nature: Electronic evidence consists of intangible electronic data and

information that cannot be perceived by ordinary senses but requires the use of computer devices and specialized software. Electronic evidence adheres to scientific reasoning and must be consistent with sound scientific principles. Similar to traditional criminal evidence seeking justice, electronic evidence aims to ascertain truth. It must align with facts and realities based on digital knowledge and evidence.(Omar Mohammed Abu Bakr bin Younis, Crimes Arising from Internet Use, Ph.D. thesis, Faculty of Law, Ain Shams University, United Arab Emirates, 2004, p97.)

The Electronic Evidence as Technical Evidence: Electronic evidence possesses a technical and technological nature, consisting of information with an electronic character that cannot be comprehended by ordinary senses, requiring the use of computer devices or reliance on technologies in general. This poses a significant challenge to the judicial system, necessitating specialized judicial expertise in this field. Judges typically rely on the opinions of experts in this domain to form their judgments.(Samah Ahmed Beltagy Moussa, Procedural Aspects of Criminal Protection on the Internet Network, Ph.D. thesis, Alexandria University, Egypt, 2010, p308.)

The Dynamic Nature of Electronic Evidence: Electronic evidence is characterized by its dynamic nature and its ability to swiftly traverse from one place to another through networks unrestricted by time and place. The

evolution of criminal evidence relies on the technological advancements inherent in its environment. Electronic evidence can effectively record and analyze information about offenders, rendering criminal investigations more efficient and manageable compared to traditional evidence.(Mamdouh Abdel-Hamid Abdel-Motaleb (2003), The Use of TCP/IP Protocol in Computer Crime Investigation: The First Scientific Conference on Legal and Security Aspects of Electronic Operations, Dubai Police Academy, April 26-28, 2003 - Dubai, United Arab Emirates, p649.)

The electronic evidence is difficult to dispose of:

Electronic evidence refers to a collection of information and data stored electronically on computers and electronic systems. This type of evidence is characterized by its difficulty in disposal, which is an essential part of its nature. When a file is deleted from a computer or the disk is formatted, data recovery techniques can retrieve deleted information, whether it's images, graphics, text, or any other type of data (Aisha Ben Qara, The Validity of Electronic Evidence in Criminal Proof: A Comparative Study, Master's thesis, Faculty of Law, Alexandria University, Egypt, 2009, p35.)

Even after data deletion, it can be repaired, restored, or displayed again, making it practically challenging to permanently dispose of. For this purpose, numerous computer programs have been developed to recover deleted

data or lost files. Additionally, attempting to delete the evidence is recorded in the computer logs, and this log can be used as evidence against the person who attempted it in the future . Therefore, it's easy to determine whether the electronic evidence has been tampered with, modified, or something added to it, using specialized applications and programs that allow users to compare it with the original version (Masira Khaled Al-Hamd (2014), Digital Guide and Its Quality Standards in Criminal Evidence, Arab Book Center, Amman, p28.)

Electronic evidence is considered one of the main features of modern technology, and historical events such as the Iran-Contra affair in the 1980s have demonstrated the power of this type of evidence. In this case, the U.S. government revealed a preference for using electronic evidence over paper evidence, as the former is difficult to dispose of. While paper evidence can be easily disposed of by shredding, electronic evidence remains retrievable and reusable even after removal. Therefore, the U.S. government initiated the implementation of a backup system for email to investigate the involvement of some officials in the office of the U.S. president through it.(AL- khashashna Tawfiq Abdullah (2021), Electronic Evidence and Its Validity in Criminal Proof, Jordanian Journal of Applied Sciences, Series of Humanities, Jordan. Volume 27, Issue 1, p6.)

The electronic evidence is distinguished by its high data storage capacity: digital

video machines, for example, can store hundreds of images, and small discs can store an entire library. Additionally, electronic evidence is characterized by its extreme dynamism, as data can swiftly move from one place to another via communication networks, transcending the constraints of time and space (Abdul Nasir Mohammed Mahmoud Fara'li, Mohammed Ubaid Saeed Al-Samari (2001), A Comparative Applied Study: The First Arab Conference on Forensic Sciences and Forensic Medicine - Criminal Evidence with Digital Evidence from Legal and Technical Perspectives, Riyadh, November 12-14, 2001, United Arab Emirates, p15.)

These unique characteristics of electronic evidence, which have made it highly distinguished, have raised concerns among the judiciary and jurisprudence regarding its ability to express the truth. This is because electronic data can be subject to manipulation, tampering, and multiple errors, necessitating the presence of conditions that grant it credibility, bring it closer to the truth, and render it acceptable as evidence in criminal courts. The criminal judge adjudicates the case according to the doctrine acquired by him. The Egyptian Court of Cassation ruled that the essence of criminal trials relies on the judge's conviction based on the evidence presented before him to convict or acquit the accused. The criminal judge enjoys full discretion in assessing all evidence presented in the lawsuit, and he can choose the evidence he trusts and cast doubt on the evidence he feels uncertain about, with the

aim of reaching the true truth. Therefore, there are conditions that must be met to accept electronic evidence before the criminal justice system, where the criminal judge retains the freedom to assess all the evidence in the lawsuit, regardless of its source, provided that it is legitimate and equivalent to the traditional criminal evidence. (Najib Hind, (2017), p166-167.)

3. The admissibility of electronic evidence in criminal proof

3.1 Ensuring the Admissibility and Reliability of Electronic Evidence

However, within the jurisdiction of Egypt, the competent court retains full discretion to assess the probative value of the elements of the claim presented for scrutiny. It assumes the role of the ultimate authority in all matters it can independently discern, provided that the subject matter under consideration does not pertain to technical issues beyond the court's capacity to adjudicate independently.

the acceptance of electronic evidence as proof before criminal justice requires several important conditions to be met.

Firstly, the electronic evidence must be admissible: meaning it must be obtained legally. The law specifies that the entity collecting the evidence must adhere to the conditions set forth in the law. Therefore, the procedures must be lawful, whether they involve issuance by the judge directly or indirectly, or statements made by the defendant during interrogation or confession, or by others after their arrest and interrogation. Obtaining and presenting evidence to the judiciary must

be done according to the methods specified in the law, ensuring a fair and accurate balance between the state's rights to punishment and the defendant's rights to provide sufficient guarantees to respect human dignity. (Samah Ahmed Beltagy Moussa, (2010), p 440.)

Of course, in cases where the rights of the defendant are violated and evidence is obtained through illegal means, the use of such evidence becomes invalid. Therefore, the court cannot rely on or consider it at any stage of the legal proceedings. Consequently, the electronic evidence presented must be valid, admissible, and compliant with the legal rules and regulations in society. It is not enough for the evidence to comply with legal rules; it must also respect human rights, treaties, international agreements, ethical, and legal rules. The judge must not establish the state's authority to punish defendants except through lawful and respectful procedures for the rights and guarantees provided by the law. Therefore, any suspicious or unreliable evidence, whether traditional or electronic, must be rejected, even if such evidence reinforces doubts about the defendant's guilt. (Rashed bin Hamad Al-Balushi (2008), Evidence in Cybercrime: The First International Conference on Information Security and Privacy in Internet Law, Sultan Qaboos University, June 2-4, 2008, Oman, p9.)

In case of violation of the suspect's rights and obtaining evidence through illegitimate means, the use of such evidence becomes invalid, and therefore the court cannot rely on it or consider it at any stage of the legal proceedings. Thus,

electronic evidence presented must be authentic, legitimate, and in accordance with the legal rules and systems applicable in society. It is not sufficient for evidence to merely comply with legal rules; it must also respect human rights, treaties, international agreements, and ethical and legal standards. The judge should only establish the authority of the state to punish suspects through legitimate and respectful legal procedures that guarantee the rights and assurances provided by the law. Consequently, any suspicious or unreliable evidence, whether traditional or electronic, must be rejected, even if such evidence strengthens doubts about the suspect's guilt. (Doueib Hussein Saber (2009), Arab Laws and Legislation Criminalizing Electronic Crimes and Society Protection, Sixth Conference, Saudi Library and Information Association, November 3, 2009, Riyadh, p19.)

In French law, criminal evidence enjoys absolute freedom; however, this does not mean that any means can be used to search for evidence, whether traditional or electronic. Instead, it must be done according to legitimate methods that respect the rights of defense, ensure the integrity of the judiciary, and protect human dignity. Although there are no direct provisions in French procedural laws regarding the principle of probity and integrity in the search for judicial truth, jurisprudence and the judiciary attach great importance to this principle, whether in the context of investigating traditional crimes or electronic crimes.

Among the examples of illicit methods that could be used to obtain criminal evidence,

including computer outputs, is the use of torture or coercion to extract information from suspects, whether physically or psychologically, to decrypt information systems. Likewise, protracted interrogations aimed at accessing specific information regarding databases or data management systems. French law indicates that invalid procedures extend their effects to subsequent procedures directly following them, whereby evidence obtained through illegitimate means, whether traditional or electronic, is rejected. In the context of digital technology usage in criminal cases, illicit methods can be exploited to acquire criminal evidence. For instance, torture or psychological pressure may be employed to obtain information from.

suspects, either through material threats or psychological coercion, such as prolonged interrogations during late hours or for extended periods to access sensitive information concerning databases or data management systems.

Moreover, deception or fraud may be used to acquire digital information, with the law indicating that illegitimate procedures in obtaining evidence render the resulting evidence void. The impact of this nullification extends to subsequent legal procedures directly affected by the unlawfully obtained evidence. Consequently, Egyptian law asserts that nullification encompasses all effects resulting from illegitimate procedures if their impacts are direct. (Najib Hind (2017), p169.)

In the French Code of Criminal Procedure prior to its amendment in 1993, Article 170 stipulated that nullity affects the flawed procedure and subsequent acts regardless of any specific link between them. This provision applied to interrogation and confrontation as outlined in Articles 111 and 114 of the law. Subsequently, in the Italian law issued in 1989, a new phrase was added in Article 191, indicating the concept of inadmissibility, whereby any violation of the legality of criminal evidence results in the rejection of such evidence, whether it is traditional or computer-generated evidence. (Hilali Abdullah (2000), *The Validity of Computer Outputs in Criminal Matters A Comparative Study*, Dar Al-Nahda Al-Arabiya for Publishing and Distribution, Amman, p126-127)

These legislations underscore the importance of respecting the legitimacy of criminal evidence and rejecting any evidence that contradicts applicable laws. If there is a violation of this legitimacy, the evidence is deemed inadmissible, irrespective of the manner of its acquisition, whether traditional or through information technology.

The electronic evidence must be conclusive: The significance of electronic evidence being reliable and conclusive is a fundamental requirement for rendering judgments of guilt or innocence in cases related to cybercrimes, whether those crimes are linked to computers or internet networks. The evidence obtained from digital devices should closely reflect the reality of the crime as much as possible, avoiding doubts and speculations. This

conclusiveness is achieved through reviewing various digital forms available, whether through direct access or displaying processed outputs on computer screens or magnetic disks, and through careful examination and review of these outputs, in addition to relying on interpretations, probabilities, inferences, and conclusions related to this evidence. Based on this, the judge can assess the evidence presented before them, ensuring its probative strength and credibility, as well as determining the link between the committed cybercrime and the accused individual. (Ali Hassan Al-Tawali (2012), *The Legitimacy of Electronic Evidence Derived from Criminal Estimation - A Comparative Study*, Security Media Center, Applied Sciences University, May 3, 2012, Bahrain, p10.)

Some laws, such as the Evidence Act in Britain of 1984, require electronic evidence to be accurate and true, and that data produced by computers be obtained in a sound manner. If this information is applied correctly and collected automatically, it is considered real evidence and is placed at the level of oral testimony, not hearsay. This necessitates relying on testimony from computer operators, programmers, and supervisors who convincingly select its operation. Consequently, there is no reasonable basis for excluding such evidence, especially if it is accompanied by a certificate confirming the computer's condition and the suitable conditions for its operation according to its design. This view aligns with the prevailing opinion in Canada, where jurisprudence considers computer outputs among the best evidence,

contributing to achieving the required certainty in criminal judgments. (AL-khashashna Tawfiq Abdullah (2021), p13.)

3.2 Admissibility of Electronic Evidence in Court Proceedings

The court mandates discussing electronic evidence in-person, with all parties present, and presenting all evidence, including computer outputs, for transparent discussion. The judge should rely on all evidence and expert reports professionally and without personal bias.

According to legal principles, electronic evidence must be discussed before the court in an oral and presentational manner. This includes all final investigation procedures conducted by the court, where evidence is presented to all parties for discussion, whether traditional or computer-generated. Witnesses must be heard again, and expert reports presented orally in the session.

Crime evidence seized must be presented to the judge personally, so they can evaluate it themselves and comprehend what they witnessed and heard in court. Oral and presentational characteristics are essential, and neglecting them leads to the nullification of legal procedures. It represents a deprivation of the right to defense by knowing the evidence presented against them, hindering their ability to refute it if desired. Relying on evidence that is not open for discussion before being considered during the pronouncement of guilt or innocence renders true justice unattainable. The principle of the necessity of discussing criminal evidence entails that

the judge must have a full opportunity to become acquainted with all the elements and evidence presented during the trial sessions. This principle applies to all types of evidence, including computer outputs considered as proof in criminal cases. Computer outputs must be presented in the trial session and discussed clearly and comprehensively before all parties to the suit, including the plaintiffs and defendants. This approach allows the judge to fully understand the evidence, assess its strength and credibility, thus aiding in making an informed decision regarding the verdict of guilt or innocence. (Rashed bin Hamad Al-Balushi (2008), Evidence in Cybercrime: The First International Conference on Information Security and Privacy in Internet Law, Sultan Qaboos University, June 2-4, 2008, Oman, p12.)

According to this principle, the judge cannot rely on any evidence or outputs without them being discussed in court sessions. This ensures that the verdict is informed and based on a full understanding of all available evidence upon which the final judgment is based.

In accordance with this provision, all evidence obtained through information technology techniques must be presented directly to the judge during the court session, not just through the case file in the preliminary investigative stage. This procedure applies to all types of technical evidence, including data and information extracted from systems and computers. Additionally, cybercrime witnesses, in all their specialties, must present their testimony in court and reintroduce their reports and findings for discussion and

examination. This procedure aims to ensure the clear and effective presentation of the truth and the revelation of justice.

Finally, all cybercrime proceeds, including evidence and materials seized, must be presented personally before the judge to ensure that the judge evaluates the case based on all available elements and evidence before him, and that his decision is based on a complete and objective understanding of the case and its components. (Rashed bin Hamad Al-Balushi (2008), p12.)

According to this principle, the judge must rely on the evidence presented before him in cases of cybercrime, and cannot rely on his personal knowledge or the opinions of others unless they are experts in the field. The experts must have submitted their reports professionally and reliably, and the judge must be satisfied with the information and analyses presented in these reports. Once the judge is convinced of the accuracy and utility of the report, he can rely on it as part of the available evidence in the case. He must consider the report alongside other evidence presented and base his decision on that. In other words, the conviction resulting from the judgment is the outcome of the judge's evaluation of all available evidence, not just the expert report alone. (Hilali Abdullah (2000), p104.)

The Admissibility of Electronic Evidence in Criminal Courts:

The mere acquisition of digital evidence and the fulfillment of all required conditions are not sufficient to consider it

as conclusive evidence for conviction. The technical nature of electronic evidence makes it susceptible to manipulation in a way that distorts the truth, without non-specialists being able to recognize such tampering. Additionally, the error rate in obtaining digital evidence procedures can be high, casting doubt on its credibility as evidence in criminal cases. However, this does not necessarily mean excluding this evidence from admissible evidence in criminal trials.

In legal systems that rely on the Latin system of proof, judges have broad authority to evaluate evidence and determine its probative value. The judge makes decisions to accept or reject evidence based on their personal conviction regarding its probative strength. Can a criminal judge, according to this system, use their discretionary power to accept or reject digital evidence based on their lack of conviction or doubt about its credibility? The judge's authority in evaluating evidence is not limited to scientific evidence, as the judge, with their legal knowledge alone, cannot understand the scientific and technological aspects of digital evidence. Additionally, digital evidence can have probative value approaching certainty, making it similar to scientific evidence in this regard.

Digital evidence meets the conditions of certainty in terms of its indication of reality, making it subject to initial acceptance by the judge without the need to verify the accuracy of the facts it proves. However, this does not mean that digital evidence is free from doubt regarding its integrity or vulnerability to tampering. Additionally,

doubts can arise about the procedures followed in collecting this evidence. (Nabil Ismail Omar (2000), The Rule of Judicial Non-Bias, Arab Journal of Security Studies, Riyadh. Volume 1, Issue 1, p90.)

The French Court of Cassation has affirmed that as long as there is no explicit legal provision excluding a particular piece of evidence, the court cannot refuse to accept this evidence, even if it is illegitimate or tainted by criminal activity. However, it is required that this evidence has undergone oral discussion in the session out of respect for the rights of the defense.

In the context of cybercrimes, the criminal judge has the authority to order an internet service provider to provide informational data related to an internet user, such as visited website addresses, downloaded files, sent or received emails, and other relevant information. Additionally, the judge has the power to request and search for electronic evidence. This includes instructing the system operator to provide necessary information to access and penetrate the system, such as disclosing secret passwords and codes for operating various programs, or assigning them to decipher encrypted data codes within the computer's memory. Furthermore, the criminal judge has the authority to order the inspection of computer systems with their components when deemed necessary and appropriate, and expertise in the field of judicial assistance plays a significant role, as it is one of the most robust aspects of the judge's handling of the presented criminal case. (Tarek Mohamed El-Gamal (2009), Digital Evidence in the Field of Criminal

Proof, Working Paper presented at the First Maghreb Conference on Informatics and Law, October 28-29, 2009, Tripoli, Libya, p25.)

When it comes to searching for electronic evidence, technical expertise plays a crucial role in navigating the legal and judicial challenges posed by advancements in technology. This expertise is essential for effectively dealing with the realm of information technology, particularly given the limited judicial understanding of computer systems and the internet. For instance, searching for information within computer systems and the internet requires specialized technical knowledge, especially when dealing with encryption and other technical methods. (Ayman Abdul Hafeez Sulaiman (2004), Legitimacy Boundaries of the Role of Police Agencies in Combating Cybercrimes, Journal of Police Research Center, Egypt. Issue 25, p384.)

However, despite this, the subject court in Egypt retains full authority to assess the probative force of the elements of the case presented for consideration. It acts as the ultimate expert in anything it can discern independently, as long as the issue at hand is not one of the technical matters beyond the court's capacity to form an opinion on its own. (Aisha Ben Qara, (2009), p193.)

In jurisdictions adopting the Anglo-Saxon legal system, typified by those following the English legal framework, a departure from the Latin system is evident. Unlike the Latin system, which upholds the freedom of proof and the discretion of the judge in assessing such evidence, this system

entrusts the legislature with delineating evidentiary standards and determining their probative value. Consequently, judges are bound by specific types or a predetermined quantity of admissible evidence as dictated by applicable legislation, irrespective of their personal convictions regarding the establishment or non-establishment of facts. Herein lies the foundation of legal certainty, rooted primarily in presuming the validity of evidence regardless of the factual reality or variances in the circumstances of the case. The role of the judge extends solely to ensuring legal compliance concerning the availability and prerequisites of evidence. If these prerequisites are not met, the judge cannot render a conviction, regardless of their personal belief, even if convinced beyond doubt of the defendant's guilt. Hence, the legal proof system distinguishes itself by vesting the legislature with the affirmative role in the evidentiary process of the lawsuit, regulating the admission of evidence, whether by specifying admissible evidence for conviction, excluding other evidence, or conferring unequivocal authority on some evidence while considering others relative.

Thus, the legal proof system distinguishes itself by attributing the affirmative role in the evidentiary process of the lawsuit to the legislature. The legislature regulates the admission of evidence, whether by specifying admissible evidence for conviction, excluding other evidence, or conferring unequivocal authority on some evidence while considering others relative (Abdul Nasir Mohammed Mahmoud Fara'li, Mohammed, (2010), p29)

In this system, the role of the judge is mechanistic, limited to ensuring the availability of evidence and its legal prerequisites. If these prerequisites are not met, the judge cannot render a conviction but must exclude the evidence, even if convinced of the defendant's guilt. The judge cannot seek the truth through other means not prescribed by the legislature, leading to a disparity between the nominal and actual value of the evidence. Despite the apparent rigidity in this system in defining legal evidence and the judge's adherence to it, some changes have occurred to make it more flexible. Some Anglo-Saxon jurisdictions have adopted a version of judicial discretion in evaluating evidence, albeit with a slightly different formulation from Latin system countries, resulting in a mixed system. Consequently, regardless of criticisms directed towards the legal evidence system, it remains predominant in Anglo-Saxon jurisdictions' laws. Hence, electronic outputs' validity faces challenges, especially with the presence of the best evidence rule and the hearsay rule.

According to the legal evidence system, which legislations prescribe acceptable evidence before the judiciary, some countries have begun enacting laws concerning computers and electronics. For instance, the United States enacted the "Computer Misuse Act" in 1990. However, this law did not address the issue of admitting computer-generated evidence before criminal courts. Instead, it relied on the Police and Criminal Evidence Act of 1984, which contained specific regulations regarding the admission of computer

outputs as evidence in criminal matters. (Aisha Ben Qara, (2009), p198.)

This law does not consider computer-generated documents or electronic documents as evidence unless complemented by reliability tests confirming the accuracy and integrity of the computer output and ensuring that the computer producing it operates efficiently and accurately.

Additionally, this law includes guidelines on how to assess the value or weight of statements extracted through a computer, considering all circumstances when evaluating computer-generated and admissible evidence, particularly considering contemporaneity. That is, whether the information relates to a matter contemporaneously provided to the

4. CONCLUSION

Through this study, we derive a set of conclusions and recommendations, namely:

Technical Challenges: Judges and investigators may face difficulty in understanding and analyzing electronic evidence due to its technical nature, which may lead to challenges in their legal conclusions and evaluations

Reliability and Trustworthiness: There may be doubts about the reliability of electronic evidence and its susceptibility to manipulation or tampering, making it difficult to accept as conclusive legal evidence.

computer or not, and whether any person accessing the computer has a motive to conceal or distort facts. (Hilali Abdullah (2000), p198.)

There appears to be a noticeable strictness in admitting electronic evidence before criminal courts, despite a series of consecutive laws attempting to keep pace with the rapid developments in electronic crimes and their evidentiary methods. Nevertheless, the matter still requires decisive resolution regarding this type of crime and evidence. This necessitates the provision of appropriate legislation and effective mechanisms for dealing with them legally and reliably. (Hisham Fareed Rostom (2010), *Procedural Aspects of Cybercrimes - A Comparative Study*, Modern Machines Library, Egypt, p178.)

Ensuring Evidence Integrity: Verifying the integrity of electronic data and preventing forgery can be challenging, jeopardizing the credibility and evidentiary strength.

Difficulty in Erasure: Electronic evidence can easily remain retrievable even after deletion, posing threats to privacy and security.

Deletion Attempt Records: Attempts to delete evidence are logged in computer records, which can be used against individuals in the future.

Complexity of Recovery: Electronic evidence recovery and technical monitoring may require additional efforts and resources, increasing costs and time consumption.

Susceptibility to Manipulation and Alteration: Electronic data may be vulnerable to manipulation and alteration, casting doubt on the credibility and reliability of electronic evidence.

Weakness in Evidence Credibility: Electronic evidence may raise concerns about its credibility and admissibility in criminal courts, negatively impacting justice.

Difficulty in Evidence Assessment: Modern electronic technologies may make it difficult for judges to adequately assess presented evidence for legal decision-making.

Illegitimacy of Evidence: Obtaining electronic evidence through illegitimate means may raise doubts about its legitimacy and validity, reducing its acceptance as legal evidence in court.

Violation of Defendant Rights: Using electronically obtained evidence through illegitimate means may violate the rights of the defendant, negatively affecting judicial integrity and its ability to achieve justice.

Judicial Reputation Damage: Illegitimate methods of obtaining criminal evidence can damage the reputation and integrity of the judiciary, adversely affecting public trust in the justice system.

Invalidity of Criminal Evidence: Failure to respect the legality of criminal evidence may lead to its rejection by the court, diminishing its value as legal proof.

Uncertainty of Electronic Evidence: Uncertainty in electronic evidence may result in its ineffectiveness or inadmissibility in criminal cases related to cybercrimes.

Failure to Discuss Criminal Evidence in Court can lead to uninformed and unjust decisions.

Failure to present computer outputs for discussion may undermine their credibility and negatively impact the course of justice.

Failure to present testimony from technology expert witnesses may lead to insufficient understanding by the judge and inaccurate decisions.

Improper reliance on technical evidence may result in inaccurate judgments and adversely affect judicial fairness.

Non-acceptance of technical reports professionally and reliably may lead the judge to rely on personal knowledge and opinions of non-experts, jeopardizing judicial decisions.

Recommendations:

Full Compliance with Legality: Legal and enforcement agencies must fully adhere to the legality of collecting criminal evidence in accordance with applicable local and international laws.

Law Enforcement: Legal authorities should ensure the enforcement of laws related to the validity of criminal evidence and reject evidence that contradicts legal standards.

Legal Personnel Training: Continuous training should be provided to judges and investigators on the importance of respecting the legality of criminal evidence and applying relevant laws.

Preserving Integrity: Legal authorities should maintain the integrity of judicial work and refrain from employing any unlawful methods in collecting criminal evidence.

Verification of Evidence Authenticity: Relevant authorities should verify the authenticity of electronic evidence and ensure its certainty by reviewing various available digital forms and examining them accurately.

Audit of Outputs: The outputs processed from electronic evidence should be audited to avoid doubts and speculations, ensuring the validity and increasing their evidential strength.

Judge's Assessment: Judges should assess the evidence presented before them, ensure its evidential strength and credibility, and base their decisions on accurate and reliable evidence.

Ensuring Linkage between Crime and Suspect: Strong linkage between electronic crime and the accused person should be ensured to achieve justice and fairness in legal proceedings.

Necessity to Simplify Procedures for presenting electronic evidence and setting clear standards for its acceptance.

Provision of specialized training for operators, programmers, and supervisors

on collecting and documenting data properly in accordance with legal requirements.

Enhancing cooperation with legislative authorities to update laws and align them with modern technologies to ensure efficient and reliable acceptance of electronic evidence.

Providing legal and technical support for lawyers and judges to understand and properly appreciate electronic evidence.

Implementing the principle of mandatory discussion of criminal evidence in all trial sessions to ensure the delivery of justice.

The necessity of presenting computer outputs before the court and discussing them thoroughly and comprehensively to ensure the enlightenment of the decision and the credibility of the evidence.

Providing appropriate training for judges and lawyers to understand the importance of discussing criminal evidence and applying it correctly during the trial.

The necessity of presenting all technical evidence and data directly and orally before the court during trial sessions to ensure the transparency of the judicial process.

Cybercrime witnesses should regularly present their testimonies and reports before the court to clarify technical matters and guide the judge in making the correct decisions.

Presenting all digital crime findings personally before the judge to ensure that their decision is based on a complete

understanding of the case and the available evidence.

The judge must evaluate all available evidence comprehensively, including expert reports, before issuing the final judgment.

5. Bibliography List :

1. Books :

Abdul Raouf Mahdi (2003), Explanation of the General Rules of Criminal Procedures, Dar Al-Ahram, Egypt.

Ahmed Fathy Sorour (2010), The Intermediary in Criminal Procedures Law, Dar Al-Nahda Al-Arabiya, Cairo.

Diaa Ali Ahmed Naaman (2011), Apparent Information Fraud and Applications: Legal Studies Series in the Field of Printed and National Paper Information, Morocco.

Hilali Abdullah (2000), The Validity of Computer Outputs in Criminal Matters - A Comparative Study, Dar Al-Nahda Al-Arabiya for Publishing and Distribution, Amman.

Hisham Fareed Rostom (2010), Procedural Aspects of Cybercrimes - A Comparative Study, Modern Machines Library, Egypt.

Mamoun Salama (2012), Criminal Procedures in Egyptian Legislation, Dar Al-Nahda Al-Arabiya, Cairo.

Masira Khaled Al-Hamd (2014), Digital Guide and Its Quality Standards in

Criminal Evidence, Arab Book Center, Amman.

2. Theses:

Abdel-Hafiz Abdel-Hadi Aabid, Criminal Proof by Indications, Ph.D. thesis, Faculty of Law, Cairo University, Egypt, 1989.

Aisha Ben Qara, The Validity of Electronic Evidence in Criminal Proof: A Comparative Study, Master's thesis, Faculty of Law, Alexandria University, Egypt, 2009.

Mohammed Taqa Faleh Rashdan Al-Hawani, Validity of Electronic Evidence as a Means of Proof in Criminal Matters (A Comparative Study between Kuwaiti and Jordanian Laws), Master's thesis, Faculty of Law, Department of Public Law, University of the Middle East, Jordan, 2015.

Omar Mohammed Abu Bakr bin Younis, Crimes Arising from Internet Use, Ph.D. thesis, Faculty of Law, Ain Shams University, United Arab Emirates, 2004.

Salama Mohammed Al-Mansouri, Application of the Principle of Spatial Conviction on Electronic Evidence, thesis submitted to fulfill the requirements for obtaining a Master's degree, Faculty of Law, Department of Public Law, United Arab Emirates University, United Arab Emirates, 2018.

Samah Ahmed Beltagy Moussa, Procedural Aspects of Criminal Protection on the Internet Network,

Ph.D. thesis, Alexandria University, Egypt, 2010.

3. *Journal article :*

AL khashashna Tawfiq Abdullah (2021), Electronic Evidence and Its Validity in Criminal Proof, Jordanian Journal of Applied Sciences, Series of Humanities, Jordan. Volume 27, Issue 1.

Ayman Abdul Hafeez Sulaiman (2004), Legitimacy Boundaries of the Role of Police Agencies in Combating Cybercrimes, Journal of Police Research Center, Egypt. Issue 25.

Nabil Ismail Omar (2000), The Rule of Judicial Non-Bias, Arab Journal of Security Studies, Riyadh. Volume 1, Issue 1.

Najib Hind (2017), Validity of Electronic Evidence in Criminal Proof, National Criminal Journal, Egypt. Volume 60, Issue 2.

4. *Seminar article:*

Abdul Nasir Mohammed Mahmoud Fara'li, Mohammed Ubaid Saeed Al-Samari (2001), A Comparative Applied Study: The First Arab Conference on Forensic Sciences and Forensic Medicine - Criminal Evidence with Digital Evidence from Legal and Technical Perspectives, Riyadh, November 12-14, 2001, United Arab Emirates.

Ali Hassan Al-Tawali (2012), The Legitimacy of Electronic Evidence Derived from Criminal Estimation - A Comparative Study, Security Media Center, Applied Sciences University, May 3, 2012, Bahrain.

Mamdouh Abdel-Hamid Abdel-Motaleb (2003), The Use of TCP/IP Protocol in Computer Crime Investigation: The First Scientific Conference on Legal and Security Aspects of Electronic Operations, Dubai Police Academy, April 26-28, 2003 - Dubai, United Arab Emirates.

Doueib Hussein Saber (2009), Arab Laws and Legislation Criminalizing Electronic Crimes and Society Protection, Sixth Conference, Saudi Library and Information Association, November 3, 2009, Riyadh.

Rashed bin Hamad Al-Balushi (2008), Evidence in Cybercrime: The First International Conference on Information Security and Privacy in Internet Law, Sultan Qaboos University, June 2-4, 2008, Oman.

Tarek Mohamed El-Gamal (2009), Digital Evidence in the Field of Criminal Proof, Working Paper presented at the First Maghreb Conference on Informatics and Law, October 28-29, 2009, Tripoli, Libya.