The Freedom of the Libyan Criminal Judge in Forming his Conviction from Digital Evidence

Maatouk Salah Eddine[1], Alfakhreeyah Hussein Abubakr[2*]

[1]Professor, Department of Private Law, University of Sidi Mohamed Ben Abdellah, Fez, Morocco. Salaheddine.maatouk@usmba.ac.ma

[2*]Vice Dean for Scientific Affairs, Faculty of Law, Omar Al-Mukhtar University, Libya PhD Student, University of Sidi Mohamed Ben Abdellah, Fez, Morocc. issebbo@gmail.com

HOW TO CITE:
Maatouk Salah Eddine , Alfakhreeyah Hussein Abubakr (2026). The Freedom of the Libyan Criminal Judge in Forming his Conviction from Digital Evidence. International Journal of Special Education, 41(8s), 436-445

COPYRIGHT STATEMENT:
Copyright: © 2026 Authors.
Open access publication underthe terms and conditions of the Creative CommonsAttribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).

ABSTRACT:
This study examines the freedom of the Libyan criminal judge in forming his conviction from digital evidence in cybercrime cases. With the rapid proliferation of electronic crimes and the increasing reliance on digital evidence in criminal proceedings, the role of the judge in evaluating electronic evidence has become pivotal. Digital evidence, characterized by its technical, scientific, and virtual nature, presents unique challenges to traditional evidentiary frameworks. This research adopts an inductive-rooted methodology, analyzing legal systems, jurisprudential opinions, and judicial rulings concerning digital evidence evaluation. The study explores the definition and characteristics of digital evidence, the judge's authority in accepting such evidence under different evidentiary systems (restricted vs. free systems), and the specific constraints on the Libyan judge's discretionary power. The findings indicate that while the Libyan legislator has adopted the free system of evidence, granting the judge broad discretion in evaluating digital evidence, this freedom is subject to significant procedural and substantive safeguards, including legality, causal connection, authenticity, logical consistency, and technical expertise. The study recommends specialized training for judges in digital forensics, the establishment of technical expert protocols, and the development of specialized judicial divisions for cybercrime cases.

Keywords: Digital Evidence, Criminal Judge, Cybercrime, Free Evidence System, Libyan Law, Electronic Proof, Judicial Discretion, Technical Expertise, Criminal Procedure, Virtual Evidence.

1. Introduction

In cases of cybercrime, digital evidence constitutes the cornerstone of proof. The criminal judge plays a crucial role in evaluating electronic evidence, and the importance of proof in the digital evidence domain is heightened because proof therein does not focus on physical facts but rather on digital evidence existing in a virtual world.

1.1 Scope of the Study

Our study will be limited to examining the evaluation of digital evidence before criminal courts and the extent of the Libyan judge's

freedom in forming his conviction in electronic crimes.

1.2 Importance of the Study

With the proliferation of electronic crimes and the trend of legislation toward enacting specific texts and laws for cybercrime, the importance of studying the extent of the criminal judge's freedom in forming his conviction from digital evidence emerges, particularly given the technical, scientific, and virtual characteristics that distinguish this evidence.

1.3 Methodology of the Study

We will adopt an inductive-rooted methodology in our study by examining the position of legal systems, jurisprudential opinions, and judicial rulings concerning the subject of the study.

1.4 Problem Statement

The subject of the study raises numerous issues, which we summarize in the following questions:

- What is digital evidence, and what are its characteristics?
- What are the proof systems in digital evidence?
- What are the limits and controls of the judge's authority in accepting digital evidence?
- What is the extent of the judge's freedom in forming his conviction in cybercrimes?

1.5 Research Plan

We will divide our research into three sections according to the following plan:

Section One: Definition and Characteristics of Digital Evidence

- First Branch: Definition of Digital Evidence

- Second Branch: Characteristics of Digital Evidence

Section Two: The Judge's Authority in Accepting Digital Evidence

- First Branch: Criminal Proof Systems

- Second Branch: Controls on the Judge's Authority in Accepting Digital Evidence

Section Three: The Libyan Judge's Authority in Evaluating Digital Evidence

- First Branch: Evaluation of Digital Evidence

- Second Branch: Presentation of Electronic Evidence by the Criminal Judge

Section One: Definition And Characteristics Of Digital Evidence

Criminal proof is defined as proving the validity of the occurrence of criminal facts represented in the material elements of the crime and the existence of its moral elements as required by law, and attributing them to the accused for committing them according to the controls established by the legislator. Digital proof, in its legal sense, is the establishment of digital evidence before the court by the methods determined by law regarding the existence of a legal fact from which its consequences arise (Al-Majbri, 2025, p. 23).

So, what is digital evidence and what are its characteristics? This is what we will answer in the first section of this research, dividing it into two branches: the first branch defines and characterizes digital evidence, and the second branch addresses the criminal judge's authority in accepting digital evidence.

First Branch: Definition of Digital Evidence

Multiple definitions have attempted to determine the term "digital evidence" due to the rapid development of the virtual environment. Some have defined digital evidence as evidence taken from computer devices, existing in the form of fields or magnetic or electrical pulses that can be collected and analyzed using special programs, applications, and technology, and presented in the form of evidence that can be relied upon before the court (Faraj, 2024, p. 73).

The International Organization of Computer Evidence defined it as every piece of information stored in the form of fields or electrical vibrations or magnetic pulses in automated processing systems or their accessories through the Internet network, and it

is extracted, collected, and analyzed according to legal and scientific procedures at any stage of investigation or trial, to produce outputs accepted by reason and logic and approved by science, aiming to prove the crime and determine guilt or innocence (Morsi, 2009, p. 213).

It has also been defined as evidence that finds its basis in the virtual world and leads to cybercrime (Qandil, 2018, p. 71).

Digital evidence is not limited only to computer devices, mobile phones, and the Internet network, but extends to any technological chip that includes data processing technology, capable of being used in criminal activities, and therefore may be a source of electronic evidence. This includes electronic game sticks through which encrypted messages can be exchanged between criminals, as well as modern home appliances such as smart refrigerators equipped with display screens, which can be used to store, display, and share illicit images (Al-Mari, 2025, p. 339).

The Libyan legislator defined criminal digital evidence in paragraph seven of Article One of the Cybercrime Law, stating: "Criminal digital evidence is the product of analyzing data from computer systems, communication networks, or digital storage devices of various types."

The U.S. Department of Justice has divided digital evidence into three categories:

1. Records stored in computers, word processing program files, and chat room messages.

2. Records created by computers, considered as computer program outputs, and mobile phone records, including paper outputs from printers, reports, and charts.

3. Records entered into computers through printers and document imaging devices, such as papers, images, and prints containing data written on Excel or Word, which have been processed through the program used (Al-Mari, 2025, p. 338).

Second Branch: Characteristics of Digital Evidence

Digital criminal evidence is distinguished from traditional criminal evidence by the following characteristics:

1. Digital evidence consists of data and information with an electronic form, non-material, requiring smart electronic devices to perceive it. Digital evidence is electronic pulses forming data recorded in digital ways that can only be read by computer (Al-Darbali & Al-Alawi, 2020, p. 112).

2. Digital evidence is virtual in its form and size; it is non-material and intangible evidence.

3. Identical copies can be extracted from digital evidence, and they have the same probative value as the original evidence.

4. Digital evidence can be recovered after deletion and its damage repaired, which may make it difficult to get rid of, and the criminal's attempt to dispose of digital evidence itself can be recorded as evidence against him, after extracting the evidence from the machine's memory (Shuaiteer & Al-Jamli, 2024, p. 75).

5. Digital evidence is ultra-fast, moving from one place to another through communication networks, and is highly affected by time (Al-Sayed & Al-Jundi, 2023, p. 46).

Section Two: The Judge's Authority In Accepting Digital Evidence

The principle that the judge relies on the evidence presented before him in the session is the cornerstone of the criminal proof system.

The prevailing rule in legislation is that the court adjudicates the case based on the evidence presented at any stage of investigation or trial, and the judge's adoption of digital evidence is not absolute, but rather he must build his judgment on extracting the truth from the legitimate evidence discussed in the session (Faraj, 2024, p. 108).

But what is the extent of the judge's authority in forming his conviction from the digital evidence

presented for discussion in the session? This is what we will address through the following two branches: the first is dedicated to studying the different criminal proof systems, and the second is dedicated to studying the controls on the judge's authority in accepting digital evidence.

First Branch: Different Criminal Proof Systems

The admissibility of digital evidence in proof varies from one legal system to another, according to the nature of the prevailing proof system. In the restricted proof system, the legislator determines the admissible evidence and specifies the conditions for its acceptance and its probative force, so the judge has nothing but to verify the conditions set by the legislator without having the freedom to evaluate the evidence. In countries that adopt the free proof system based on the principle of the judge's freedom in forming his conviction, the judge is not restricted to accepting digital evidence except that it must have been obtained in a legitimate manner, observing formal and substantive conditions during the search for evidence (Al-Mari'i, 2024, p. 58).

There are different criminal proof systems that vary according to legislation, including:

The Restricted Legal Proof System: In this system, the law determines the evidence that the judge relies on in his judgment. In this system, the judge does not search for the truth, but rather the extent to which the evidence determined by the legislator applies to the facts, without his conviction having any legal value.

The Free Proof System: In this system, the judge is not restricted to certain proof evidence, but he may build his judgment on any evidence presented before him in the session. The judgment here is based on the judge's freedom in forming his conviction and reaching certainty and conviction with evidence of conviction without restriction, except in certain cases excluded by law. Most contemporary legislation adopts this system, including French, Iraqi, Egyptian, and Libyan legislation, which established the principle of the judge's freedom in forming his conviction in criminal proof matters. The judge exercises his discretionary authority in evaluating the facts of the case, their circumstances, and evidence of conviction and innocence alike, to reach the decisive criminal evidence that leads to revealing the truth (Shwani, 2017, p. 27).

Second Branch: Controls on the Judge's Authority in Accepting Digital Evidence

The judge's adoption of digital evidence is not absolute, but rather the evidence must be built on certain controls so that it can be accepted by the court. These controls are as follows:

1. Causal Connection: The connection of the evidence to the fact. It is required that the digital evidence have a direct relationship with the criminal act that is the subject of the accusation; there is no benefit from data that proves nothing or denies nothing.

2. Authenticity and Integrity of Evidence: The original version of the evidence must be preserved and the chain of custody documented. Copies or duplicated outputs are not accepted unless it is proven that the data remained preserved without modification. The judge may not base his judgment on mere inferences, but he must base his judgment on evidence, and there is no objection to the court reinforcing the available evidence with inferences (Arhuma, n.d., p. 154).

3. Requirements of Reason and Logic: The judge's conclusion of the truth must be consistent with the requirements of reason and logic. Although the criminal judge is free in forming his conviction by extracting legal facts and the facts of the case, this is conditional on the judge extracting the evidence according to what the logical sequence of matters requires without contradiction with the requirements of sound reason and logic (Shwani, 2017, p. 239).

4. Legitimacy: The principle of legitimacy of digital evidence means that the competent authority that collected the evidence must have

complied with the conditions specified by law in this regard. The acceptance of digital evidence requires that it have been collected in legitimate ways that respect privacy and the law. For criminal evidence to be legitimate, the procedural act that resulted in the evidence must be valid, fulfilling the substantive and formal conditions set by the law for the validity of the procedure; otherwise, the procedure is void and so is the evidence resulting from it (Qandil, 2018, p. 100).

5. Corroboration of Criminal Evidence: The criminal judge must build his conviction and conviction judgment on the totality of evidence, as criminal evidence complements each other. The condition of corroboration of evidence is necessary in the case of a conviction judgment. Accordingly, if a defect is found in one of the evidence of the case, it affects the inference from all that evidence collectively, making it impossible to determine the extent of the effect of the invalid evidence on the court's conviction (Arhuma, n.d., p. 166).

6. Technical Expertise: Due to the scientific nature of digital evidence, the judge should seek assistance from an accredited technical expert to interpret the digital content and evaluate its credibility when the judge does not have the authority to evaluate the scientific technical value of digital evidence that requires special technical and technological knowledge.

In this regard, the Egyptian Court of Cassation ruled that: "There is no importance to the appeal against the judgment on the grounds that it relied in conviction on a report of emptying the recorded tapes, despite the investigator's inability to determine the content of the recorded dialogue from which the agreement on bribery is inferred, as long as the judgment was not based on this report alone, but was based on the statements of proof witnesses and a live report, which are evidence that collectively lead to what was intended from them and are productive in completing the court's conviction and reassurance of what it concluded" (Shwani, 2017, p. 242).

Section Three: The Libyan Judge's Authority In Evaluating Digital Evidence

The Libyan legislator did not dedicate special rules in the Cybercrime Law texts for presenting digital evidence before the court, but rather subjected it to the general rules of proof established in the Libyan Criminal Procedure Law. It is understood from this that digital evidence is treated like any other criminal evidence, and the court must verify the availability of acceptance and persuasion conditions in it, not merely because it is electronic.

We will address through the following two branches the study of evaluating digital evidence in the first branch, and presenting digital evidence by the criminal judge in the second branch.

First Branch: Evaluation of Digital Evidence

The general rule is that the court evaluates all evidence, including digital evidence, according to its discretionary authority, based on the principle of the judge's freedom in forming his conviction, and based on the extent of its connection to the criminal act, and the integrity of the method of obtaining it. It is not automatically obligated to accept digital evidence, but exercises its authority in evaluation according to the general rules established in the Criminal Procedure Law. This digital evidence is subject to the authority of reason and logic. The principle of the judge's freedom in forming his conviction means that the judge has the freedom to evaluate the evidence presented before him according to his personal conviction, so he may derive his conviction from it and rely on it in the judgment he reaches. If he is not reassured by it and finds it insufficient, he may reject the electronic evidence like other traditional evidence (Qandil, 2018, p. 151).

The court may reject digital evidence if it becomes clear to it that it was obtained in an

uncontrolled or illegitimate manner, such as privacy violation or the absence of judicial permission, or if it is not clearly related to the criminal act.

The judge may rely on digital evidence as long as it has been presented in a legal framework, accompanied by what proves its technical credibility, such as official reports or electronic seizure minutes, where the legislator permitted the judge to rely on digital evidence by defining it in Article One of the Law (Shuaiteer & Al-Jamli, 2024, p. 95).

Based on the foregoing, the judge's authority in accepting digital evidence is a discretionary authority linked to the guarantees of legitimacy and justice, requiring him to investigate the validity of the evidence, its origin, and the circumstances of obtaining it, and to seek assistance from experts, and not to rely on his personal intuition or private technical knowledge. He may not base his judgment on his emotions, whims, and desires, for conviction is a conscious mental act whose source is reason, not emotion.

The judge must seek assistance from technical experts in matters that require technical knowledge that he cannot comprehend, and he may not dismiss the expert opinion in these matters except for reasonable reasons. In this regard, the Libyan Supreme Court ruled in its criminal appeal No. (66/18 Q) that: "The judge's seeking assistance from experts in technical matters that he cannot comprehend requires him to place the experts' opinion in technical matters and not to dismiss their opinion except for acceptable and convincing reasons" (Al-Salabi, 2010-2011).

The original principle is that the judge is free in forming his conviction, so there are no specific equations for how the judge exercises his conviction formation, because conviction is not a mathematical process but rather a mental state based on the requirements of reason and logic that the judge reaches through scrutiny and examination of legitimate criminal evidence.

Although the general principle is that the criminal judge derives his conviction from any evidence he is reassured by, because the principle in criminal law is the judge's freedom in forming his conviction, this principle is subject to exceptions in cases where the legislator specifies certain evidence in proof in some crimes, where the judge in these crimes may only adopt the evidence specified by the legislator as proof evidence in hudud crimes (Qandil, 2018, p. 160).

Second Branch: Presentation of Electronic Evidence by the Criminal Judge

Presentation of electronic evidence means that the judge displays the data and digital outputs before the adversaries in a public session, so that each party has the opportunity to examine and discuss them.

This procedure is considered a fundamental condition for the integrity of the judgment; for criminal jurisprudence affirms that the judge may not rely on evidence that has not been presented for discussion. For the presentation of electronic evidence to be correct, the conditions for accepting electronic evidence must be observed:

First: Presenting the Original Copy with a Matching Copy

Digital evidence is presented in its original form or its content is presented in writing if the nature of the data permits, with an accurate copy preserved in the case file to ensure the possibility of referring to it.

The denial of printed screenshots of messages that are the subject of the incident cannot be claimed, and in this regard, the Egyptian Court of Cassation ruled that: "Since the existing papers do not apply to the legal description of the customary paper issued by individuals, they are outputs of an electronic screen that is the WhatsApp application for social communication on the international information network, the Public Prosecution examined their original by inspecting the complainant's phone and

emptying their contents, and the expert examined them, whom the court is reassured by his report and adopts it, so the denial of these documents is misplaced and the court rejects it" (Appeal No. 4 for the year 89 Q, session 19/10/2019) (Al-Mari, 2025, p. 32).

Second: The Digital Evidence Must Be Certain

The electronic evidence must be certain so that the absolute truth can be reached through it. The criminal judge must be convinced of the conviction evidence with a decisive certainty that leaves no room for doubt. Electronic conviction evidence, like other criminal evidence, is required to be not subject to conjecture and probability, otherwise the judge must rule for acquittal if he does not reach the stage of certainty and absolute conviction.

The judge's conviction of electronic evidence is achieved through what he concludes from examination, scrutiny, and electronic knowledge, and he may seek technical expertise that plays a prominent role in digital proof, to ensure the integrity of the evidence and the correctness of the procedures followed in obtaining it. Digital evidence can be subject to tampering and appear as if it were an original copy, which may require seeking assistance from information technology experts to ensure that the evidence has not been tampered with and to ensure that there is no error in extracting the evidence (Shuaiteer & Al-Jamli, 2024, p. 113).

The judge must seek assistance from technical experts in matters that require technical knowledge that he cannot comprehend, and he may not dismiss the expert opinion in these matters except for reasonable reasons. In this regard, the Libyan Supreme Court ruled in its criminal appeal No. (66/18 Q) that: "The judge's seeking assistance from experts in technical matters that he cannot comprehend requires him to place the experts' opinion in technical matters and not to dismiss their opinion except for acceptable and convincing reasons" (Al-Salabi, 2010-2011).

Third: Oral Discussion

The principle of the necessity of discussing criminal digital evidence in the session requires that the digital outputs be presented in the session, and the adversaries be granted the right to examine and discuss them. The criminal judge must present every piece of evidence in the case for discussion before the adversaries, including the discussion of electronic evidence, in application of the principle of oral argumentation. This is done by providing the opportunity for the parties to the case to examine the evidence and granting the defense sufficient time to examine the evidence and summon a technical expert if necessary. The judge may not base his conviction on evidence that has not been presented for discussion in the trial sessions, otherwise the evidence is invalid and may not be relied upon in the judgment. The rationale for this is to give the accused his right to defend himself against the evidence, in addition to the fact that discussing the evidence in the session may affect the judge's conviction of the criminal evidence or not.

According to the principle of public discussion, criminal digital evidence must be discussed in the session and the digital outputs must be presented in the session, and the adversaries be granted the right to examine and discuss them and raise the technical defenses they have. The principle of oral argumentation provides the opportunity for the other party to examine the evidence, and the judge may not base his judgment on personal information he obtained outside the scope of the case presented, but he must build his judgment on evidence that has been presented and discussed in the session (Al-Frayhat, 2024, p. 79).

The judge of the merits must break the seal of the recordings and listen to them in the session in the presence of the adversaries and allow them to present their defense on them, and this procedure is one of the fundamental rules in criminal procedures, so it must be carried out even if the adversaries do not request it.

Despite the connection of the public discussion procedure to public order, we find that a trend in the judiciary departs from this rule of breaking the seal of recordings and rules that it is not connected to public order. Among this, we find that the Egyptian judiciary departed from this rule in its rulings related to breaking the seal of recordings, as the Egyptian Court of Cassation ruled: "Since it is clear from examining the minutes of the trial sessions that the appellant or his defenders did not request the court to listen to the recordings, he has no right to criticize the court for refraining from carrying out a procedure that was not requested from it and that it did not see a need to carry out" (Cassation, February 21, 2010, Rulings of the Egyptian Court of Cassation, Year 61, No. 24, p. 158) (Shwani, 2017, p. 252).

Fourth: The Judge Must Derive His Conviction from a Legally Valid and Legitimate Procedure

The judge must commit to excluding any evidence obtained in illegal ways or whose content has been tampered with, in application of the principle of procedural legitimacy.

Procedural legitimacy means adhering to the provisions of the law and working within its framework during the search for criminal evidence, to ensure the protection of individuals' fundamental rights. The judge must derive the evidence from legitimate procedures, and the legitimacy of the evidence means that the law permits the judge to rely on the evidence in forming his conviction, and the law does not permit evidence obtained by exceeding the controls and procedures of searching for evidence. All legislation, including Libyan legislation, prohibits resorting to means aimed at extracting criminal evidence by infringing on individuals' freedom, safety, threatening them, or using violence against them, or violating their sanctity and privacy (Al-Majbri, 2025, p. 51).

Therefore, the judge must ensure the integrity of the technical procedures used in obtaining digital evidence. For example, he may not rely on digital evidence obtained from a computer search outside the state's territory except based on judicial assistance and delegation procedures, in application of judicial delegation agreements or reciprocity (Shuaiteer & Al-Jamli, 2024, p. 121).

The assessment of the extent of the connection of the evidence to the invalid procedure is a substantive matter that returns to the court of merits, and in this regard, the court of merits ruled that: "Whenever the invalidity of any procedure is established, it includes all the direct consequences resulting from it without affecting the remaining procedures that are not based on it, so it rules the invalidity of the evidence derived from it only without affecting the remaining procedures" (Criminal Appeal No. 11/20 Q, session 14/05/1974, Supreme Court Magazine, Year 10, No. 4, p. 313).

The extent of the legitimacy of digital evidence raises many issues, including the question related to the legitimacy of evidence derived from visual recording without the owner's permission in criminal proof. In other words, is it permissible for the judge to rely on evidence obtained from hidden or apparent recording in a public place if the recording was done without the criminal's permission? Is it permissible for the criminal to claim the illegitimacy of the evidence for taking pictures without his permission?

From the applications of Egyptian jurisprudence in visual recording in public places, the Cairo Criminal Court ruled on 5/3/2013 to imprison one of the Central Security officers for three years in a case whose facts are summarized in an individual taking pictures with his smartphone equipped with a camera of one of the Central Security officers using a shotgun during the dispersal of demonstrations, and the voice of one person beside him saying that the bullet came in the eye of one of the demonstrators. From this ruling, it is clear to us the integrity of the evidence obtained from hidden visual recording in public places (Al-Mari, 2025, p. 855).

Fifth: The Principle That the Judge May Not Judge Based on His Knowledge

The question arises regarding the probative value of digital data published on the international information network about the cybercrime that is the subject of the case presented: Is it permissible for the judge to rely on it as evidence that he obtained himself from the Internet? Or does this contradict with the principle that the judge may not judge based on his knowledge?

It is known that the judge may not judge based on his personal information and his transformation from a judge to a witness, but this does not prevent him from judging based on his knowledge of general scientific knowledge that does not require proof.

Sixth: Preparing a Detailed Report

The presentation of evidence must be recorded in the session minutes, with a description of the tool used and the results obtained, which is called the reasoning of judgments to ensure the Supreme Court's oversight of the integrity of the procedures. With these mechanisms, electronic evidence takes its place in the criminal trial and becomes part of the elements of judicial conviction while guaranteeing the rights of defense.

Conclusion

First: Results

1. Digital evidence extends to any technological chip that includes data processing technology, capable of being used in criminal activities.

2. In the restricted proof system, the legislator determines the admissible evidence and specifies the conditions for its acceptance and its probative force, so the judge has nothing but to verify the conditions set by the legislator without having the freedom to evaluate the evidence. If digital evidence is not specified, the judge may not adopt it.

3. In countries that adopt the free proof system based on the principle of the judge's freedom in forming his conviction, the judge is not restricted to accepting digital evidence except that it must have been obtained in a legitimate manner.

4. The principle that the judge may not rely on evidence that has not been presented for discussion in the session is a principle agreed upon in both restricted and free proof systems.

5. The criminal judge must be convinced of digital evidence for conviction with a decisive certainty that leaves no room for doubt.

Second: Recommendations

1. We recommend that legislation adopting the restricted proof system specify digital evidence as admissible evidence in cybercrimes and determine its nature and conditions for acceptance.

2. We recommend that the judge seek assistance from technical experts in digital evidence that requires technical knowledge that he cannot comprehend, and not to dismiss the expert opinion in these matters except for reasonable reasons, especially with the lack of qualified human cadres available to adjudicate these matters among judicial bodies.

3. We recommend the specialization of the criminal judge in electronic cases, especially given what these crimes require of special technical and scientific knowledge.

4. We recommend continuous training for judges in the field of digital technology, so that the judge builds his judgment on certainty and conviction, and criminals do not escape punishment by affecting the judge's conviction due to his lack of technical knowledge.

References

Al-Darbali, S., & Al-Alawi, A. (2020). Aḥkām jirimat al-qaḍf ʿabra mawāqiʿ al-tawāṣul al-ijtimāʿī al-fīsbūk fī al-fiqh al-Islāmī wa-al-tashrīʿ al-Tūnisī [Rulings of the crime of defamation through Facebook social media in Islamic jurisprudence and Tunisian legislation]. Majmaʿ al-Aṭrash li-Nashr al-Kutub al-Mukhtaṣ wa-Tawzīʿih, Tunis.

Al-Frayhat, I. H. (2024). Al-masʾūliyyah al-jināʾiyyah li-jarāʾim ibtizāz al-ashkhāṣ iliktrūniyyan fī ḍawʾ qānūn jarāʾim al-ibtizāz al-shakhṣī iliktrūnī al-Urdunī wa-al-Tūnisī (dirāsah muqāranah) [Criminal responsibility for electronic blackmail crimes in light of the Jordanian and Tunisian electronic personal blackmail crimes law (comparative study)]. Majmaʿ al-Aṭrash li-Nashr al-Kitāb al-Mukhtaṣ wa-Tawzīʿih, Jordan.

Al-Majbri, F. M. J. (2025). Qubūl al-dalīl al-iliktrūnī amām al-qāḍī al-jināʾī [Acceptance of electronic evidence before the criminal judge]. Dār Jīn lil-Ṭibāʿah wa-al-Nashr, Libya.

Al-Mari, B. (2025). Asʾilah wa-ajwibah fī jarāʾim al-mūbāyl wa-al-intirnīt wa-taqniyyat al-maʿlūmāt [Questions and answers in mobile, internet, and information technology crimes]. Dār al-Ahrām lil-Nashr wa-al-Tawzīʿ wa-al-Iṣdārāt al-Qānūniyyah.

Al-Mari, B. (2025). Jarāʾim al-intirnīt wa-faqan li-qānūn mukāfaḥat jarāʾim taqniyyat al-maʿlūmāt wa-al-qawānīn al-jināʾiyyah al-ukhra [Internet crimes according to the law combating information technology crimes and other criminal laws]. Dār al-Ahrām.

Al-Mari'i, A. L. (2024). Al-adillah al-raqmiyyah al-mutaḥaṣṣalah min al-taftīsh al-jināʾī al-iliktrūnī [Digital evidence obtained from electronic criminal search]. Dār al-Ahrām.

Al-Salabi, F. Y. (2010-2011). Al-mawsūʿah al-shāmilah li-mabādiʾ al-maḥkamah al-ʿulyā al-Lībiyyah [The comprehensive encyclopedia of the principles of the Libyan Supreme Court]. Appeal No. 66/18 Q, Criminal Principles, Section Four.

Al-Sayed, A. M., & Al-Jundi, M. (2023). Al-jarāʾim al-sibrāniyyah bayn al-naẓariyyah wa-al-taṭbīq [Cybercrimes between theory and application]. Dār al-Saḥāb.

Arhuma, M. M. (n.d.). Al-wasīṭ fī sharḥ al-aḥkām al-ʿāmmah li-qānūn al-ijrāʾāt al-jināʾiyyah al-Lībī [The mediator in explaining the general provisions of the Libyan Criminal Procedure Law]. (Part Two: Trial and Appeal in Judgments). First Edition.

Faraj, A. (2024). Sulṭat al-qāḍī al-jināʾī fī taqdīr al-dalīl al-iliktrūnī [The authority of the criminal judge in evaluating electronic evidence]. Dār al-Maṭbūʿāt al-Jāmiʿiyyah.

Morsi, M. M. (2009). Al-taḥqīq al-jināʾī fī al-jarāʾim al-iliktrūniyyah [Criminal investigation in electronic crimes]. Maṭābiʿ al-Shurṭah, First Edition.

Qandil, A. A. (2018). Al-wasāʾil al-iliktrūniyyah wa-dawruhā fī al-ithbāt al-jināʾī [Electronic means and their role in criminal proof: Comparative study]. Dār al-Jāmiʿah al-Jadīdah.

Shuaiteer, J. J., & Al-Jamli, T. M. (2024). Al-tajrīm wa-al-ithbāt fī al-wasaṭ al-iftrāḍī [Criminalization and proof in the virtual environment: Cybercrime and electronic evidence in Libyan law]. Dār al-Faḍīl lil-Nashr wa-al-Tawzīʿ, First Edition.

Shwani, D. K. (2017). Ḥujiyyat al-ṣawt wa-al-ṣūrah fī al-ithbāt al-jināʾī [The probative value of sound and image in criminal proof: Comparative study]. Dār al-Jāmiʿah al-Jadīdah.

Supreme Court of Libya. (1974). Criminal Appeal No. 11/20 Q, session 14/05/1974. Supreme Court Magazine, 10(4), 313.