Journal of Politic and Law **Volume: 18/ N°: 02 (2026), p.p279-292**

Digital Evidence Engineering: Towards an Integrated Legal and Technical Vision for Proof in the Virtual Environment

هندسة الدليل الرقمي: نحو رؤية قانونية وتقنية متكاملة للإثبات في البيئة الافتراضية

BOUDJELLAL Abdelkader[1*]
Laboratory of Development Strategies in the Border Regions of the Great South, University of Tamanrasset (Algeria), a.boudjlal@univ-tam.dz

BERRADI Ahmed
University of Tamanrasset (Algeria), beradi.ahmed@univ-tam.dz

Received: 11/05/2026 ***Accepted: 30/05/2026*** ***Published:02/06/2026***

Abstract :
Criminal proof in cybercrimes presents significant legal challenges because digital evidence is intangible, easily modified, and transcends physical borders. This forces a judicial dilemma between 'Free Proof' systems, based on discretionary conviction, and 'Restricted Proof' systems, which require strict technical compliance. Furthermore, the fluidity of cloud-based crime scenes complicates traditional search and seizure operations. To address these issues, states must modernize their legal frameworks by training specialized investigators and updating procedural laws for expedited data preservation. Crucially, enhancing international judicial cooperation is vital to overcome jurisdictional barriers in global cyberspace. These reforms are essential to ensure the credibility of digital evidence and prevent impunity in an increasingly complex technological landscape.
Keywords:*Expedited Digital Preservation; Digital Footprint; Anti-Digital Forensics; Bit-stream Imaging; Digital Chain of Custody.*

ملخص:
يطرح الإثبات الجنائي في الجرائم السيبرانية تحديات قانونية جسيمة؛ نظراً لطبيعة الدليل الرقمي غير المادية، وسهولة تعديله، وتجاوزه للحدود الجغرافية. ويفرض هذا الواقع مأزقاً قضائياً بين نظم 'الإثبات الحر' القائمة على الاقتناع الوجداني للقاضي، ونظم 'الإثبات المقيد' التي تشترط امتثالاً تقنياً صارماً. وعلاوة على ذلك، فإن الطبيعة المتغيرة لمسارح الجريمة القائمة على الحوسبة السحابية تُعقّد عمليات التفتيش والضبط التقليدية.
ولمواجهة هذه الإشكاليات، يتعين على الدول تحديث أطرها القانونية من خلال تأهيل محققين متخصصين وتطوير القوانين الإجرائية لضمان 'الحفظ السريع للبيانات'. كما يُعد تعزيز التعاون القضائي الدولي أمراً حيوياً لتجاوز عقبات الاختصاص القضائي في الفضاء السيبراني العالمي. وتُعتبر هذه الإصلاحات ضرورية لضمان حجية الأدلة الرقمية ومنع الإفلات من العقاب في ظل مشهد تكنولوجي يزداد تعقيداً.
كلمات مفتاحية: التحفظ الرقمي السريع؛ البصمة المعلوماتية؛ مكافحة التحقيق الرقمي؛ النسخ المتطابق؛ سلسلة الحيازة الرقمية.

I- Introduction:

[1]***BOUDJELLAL Abdelkader.***

The technological revolution has brought about a radical shift in the lives of societies, as human activity has migrated to cyberspace, leading to the emergence of novel criminal patterns that were previously unknown. These crimes are characterized by being trans-border and unrecognizing of geographical barriers, which has put traditional rules of justice in a race against time to keep pace with this rapid development and to adapt physical evidence to suit the virtual environment.

The special nature of cybercrime necessitates reliance on evidence of the same technical nature, as digital acts cannot be proven except through advanced technological means. Criminal proof in this context depends on digital evidence as a decisive element in linking the perpetrator to their criminal activity flowing through global networks.

The primary problem centers on how to extract digital evidence and ensure its legitimacy in the absence of a tangible physical entity and the ease of erasing digital traces. The fundamental question arises regarding the adequacy of traditional procedural texts in dealing with evidence characterized by fluidity and volatility, and how a criminal judge can form their certain conviction based on invisible electronic pulses.

Furthermore, the problem raises legal challenges related to the duality of the crime scene and the conflict of cross-border judicial jurisdiction. The study raises a question about how to reconcile the requirements of efficiency in digital investigation with the necessity of protecting individuals' privacy, which is constitutionally guaranteed, especially when dealing with data stored in the "cloud" or international systems.

The theoretical importance lies in the attempt to fill the legislative vacuum and clarify the newly developed concepts of digital evidence and distinguish it from traditional evidence. The study contributes to laying solid legal foundations that help the legislator draft texts compatible with the scientific and technical nature of proof in the digital age, ensuring the accuracy of judicial rulings.

As for the practical importance, it is manifested in providing a practical guide for search and investigation officers and judges on how to deal with information devices and networks as tools for proof. This study helps in enhancing the efficiency of security agencies in facing "Anti-Digital Forensics" techniques resorted to by professional criminals to hide their identities and destroy evidence.

The research primarily aims to demonstrate the technical specificity and intangible nature of digital evidence in light of ongoing technical developments. It also seeks to define the legal and objective conditions for accepting this evidence before the judiciary, to ensure that proof is based on sound technical procedures that do not accept doubt or interpretation.

In addition, the study aims to review international cooperation mechanisms in seizing cross-border digital evidence and explaining the role of technical expertise in analyzing encrypted data. The research seeks to provide proposals for developing the procedural system to ensure the speed of access to evidence before its technological disappearance.

The study relied on the descriptive-analytical method to describe the nature of digital evidence and its technical characteristics accurately. This method allows for deconstructing the elements constituting digital data and analyzing how they transform from mere magnetic pulses into criminal evidence acceptable to logic and reason.

The comparative method was also used to monitor the positions of various legislations and jurisprudential opinions in dealing with digital proof issues. This method helped in identifying legal loopholes in national systems compared to international agreements, which

allowed for reaching results and practical recommendations to enhance the probative value of digital evidence.

This study has been divided into two main chapters: the first chapter deals with the technical nature of digital evidence and its legal challenges, focusing on its qualitative characteristics and its probative value in the face of traditional evidentiary systems.

Meanwhile, the second chapter is devoted to the technical procedures for investigation and how to practically confront obstacles, through adapting inspection and search procedures to the digital environment. The research concludes by addressing the obstacles of judicial jurisdiction and the necessity of activating international technical cooperation to ensure that cybercriminals do not escape punishment.

Chapter One: The Technical Nature of Digital Evidence and Its Legal Challenges

Section One: Qualitative Characteristics of Digital Evidence

Digital evidence is defined as that information obtained through legal and scientific procedures through the translation of computational data stored in computer devices and their accessories; it is evidence that finds its basis in the virtual world and clearly leads to the disclosure of the committed crime. The technical nature of this evidence is evident in its being extracted from a medium that the senses cannot perceive directly, but rather requires technological means to extract and present it in an intelligible form[1].

Digital evidence fundamentally consists of magnetic or electrical pulses that can be collected and analyzed using advanced technological programs and applications. These are digital components aimed at providing information in various forms such as text, images, or drawings. This transition from invisible pulses to readable forms is what grants digital evidence its unique characteristics and makes it radically different from traditional physical evidence that relies on tangible entities[2].

Cybercrime is considered one of the "soft" and tempting crimes for criminals because it takes place in a high-speed digital environment, does not require physical effort, but rather depends on technical intelligence and the ability to manipulate data. These characteristics dictate that digital evidence must be scientific evidence of the first degree, as its extraction requires a technical environment similar to the environment that produced it, necessitating the use of appropriate computer programs to view it.[3]

The technical nature of the evidence is manifested in its being a series of records automatically created by devices, such as call logs or bank card records, or records saved by human input such as email messages. This diversity in evidence sources—between purely automated and mixed—adds complexity to the proof process, where digital paths must be traced with extreme accuracy to ensure the loss of any digital trace left by the perpetrator.[4]

---

[1]Masoud bin Humaid Al-Maamari, "Digital Evidence for Proving Cybercrime," Kuwait International Law School Journal, Special Supp., no. 3 (2018), 193.

[2]Merghad Shahira and Haddad Issa, "The Admissibility of Electronic Evidence Before Criminal Courts," Journal of the Department of Legal and Political Research and Studies, 7, no. 2 (2023), 297.

[3]Thunayyan N. Al-Thunayyan, "Proving Cybercrime: A Rooted and Applied Study" (Master's thesis, Naif Arab University for Security Sciences, Saudi Arabia, 2012/2013), 22.

[4]Labiad Adel and Nezli Bouchra, "Proving Cybercrime" (Master's thesis, University of Ouargla, Algeria, 2017/2018), 29.

Digital evidence is also characterized by being invisible and unreadable by the naked eye in its raw state; it leaves no tangible physical trace like traditional fingerprints or bloodstains, but rather is mere pulses flowing within information systems. This absence of an external physical entity makes the process of monitoring and seizing it a great challenge requiring high technical efficiency from the search and investigation authorities to reach the judicial truth.[1]

Subsection One: The Intangible and Scientific Nature of the Evidence

The intangible attribute is the most prominent feature of digital evidence, as it does not occupy space in a vacuum like paper documents, but is rather a moral entity stored on magnetic or optical media. This type of evidence cannot be touched by hand or dealt with in its digital state except through its translation into an intelligible human language, which makes it "technical evidence" that falls outside the scope of traditional physical evidence[2].

Digital evidence is scientific evidence by nature because it is the product of computer and communication science and cannot be obtained except by following specific scientific and technical methods. The virtual world in which the evidence exists is a world prepared by specialists; therefore, the decryption and analysis of its contents are only done through parallel technical tools, which makes it enjoy high scientific credibility if dealt with according to correct standards.[3]

Studies confirm that digital evidence is characterized by being an "electronic trace" consisting of binary signals (0-1) called "Bits," which is the basic unit for building information inside a computer. This microscopic digital nature makes the evidence resistant to traditional destruction but easy to erase technologically, which adds a scientific character to the search and investigation and makes it impossible for non-specialists to deal with it without causing damage to its integrity.[4]

Criminal jurisprudence suggests that digital evidence represents an advanced stage of physical evidence, as it can be converted into a tangible physical form by printing it or extracting it onto solid media. However, it retains its scientific characteristics that impose on the judiciary not to be satisfied with the paper report, but rather the necessity of reviewing the original digital environment to estimate its probative value with certainty.[5]

Scientific evidence for digital evidence appears clearly when talking about the "Digital Footprint" left by the user when connecting to the network. These are information traces that cannot be easily erased even using ordinary deletion tools. This scientific nature requires the use of specialized programs to recover deleted data, making digital evidence elusive to final loss if technical expertise is available.[6]

Subsection Two: The Volatile and Trans-border Nature of the Evidence

Digital evidence is characterized by the feature of rapid change; it is fragile evidence susceptible to modification or deletion in fractions of a second, whether by the perpetrator to

---

[1]Al-Tayeb Al-Baraka and Hadj Soudi Mohamed, "The Problem of Proof in Cybercrimes," Afaq Ilmiya Journal, 11, no. 1 (2019), 269.
[2]Al-Maamari, supra note 1, 197.
[3]Shahira and Issa, supra note 2, 312.
[4]Seksek Mohamed, "Criminal Proof in Cybercrimes" (Master's thesis, University of Djelfa, Algeria, 2021/2022), 14.
[5]Thunayyan N. Al-Thunayyan, supra note 3, 15.
[6]Al-Baraka and Mohamed, supra note 5, 272.

hide the features of their crime or as a result of a technical error during the seizure process. This digital fluidity makes the time factor a decisive element in criminal proof, as any delay in seizing the evidence may lead to its permanent loss or the loss of its legal value due to unauthorized intervention.[1]

One of the most important challenges posed by digital evidence is its trans-border nature, as the crime may be committed in one country and its effects appear in a second country, while the digital evidence is stored in servers belonging to a third country. This digital globalization breaks the barriers of regional sovereignty and makes it difficult for national investigative authorities to access the evidence without intensive international cooperation and bilateral or collective agreements.[2]

Cybercrimes are "international" crimes par excellence, as their perpetrators exploit the Internet to store their data in information systems outside the jurisdiction of the state in which the crime occurred to thwart the investigation. This leads to the emergence of complex legal problems related to spatial jurisdiction and the extent of the legitimacy of cross-border search, which is known as "Remote Search" or trans-border search.[3]

The speed of data transfer across global networks makes digital evidence a highly dynamic piece of evidence; a single piece of evidence can be distributed across more than one information system in geographically distant locations. This digital dispersion requires investigators to use advanced tracking techniques such as (IP Address) to trace the evidence in its international paths and ensure that the criminal does not escape punishment by resorting to safe digital havens.[4]

Criminal proof in this context faces the dilemma of "evaporating evidence," as digital data by its flexible nature can disappear with the mere cutting of the electric current or the use of self-destruction programs. Therefore, modern laws have begun to move towards establishing "Expedited Preservation" of data to ensure its retention and non-alteration until international judicial assistance procedures are completed to obtain it officially.[5]

Section Two: The Probative Value of Digital Evidence in the Face of Traditional Evidentiary Systems

The probative value of digital evidence raises profound legal problems when compared to traditional written evidence, as classical rules of evidence required the presence of a paper support and a handwritten signature for the document to be considered complete proof. However, legislative development has forced the recognition of the probative value of electronic documents, provided that the identity of the issuer can be verified and that they were prepared and preserved under conditions that guarantee their integrity from tampering.[6]

Under modern laws, digital evidence has come to enjoy the same evidentiary force as physical evidence, provided it is extracted in a legitimate manner and not in violation of constitutional provisions or procedural laws. Its value depends on the ability of technical

[1] Al-Maamari, supra note 1, 199.
[2] Shahira and Issa, supra note 2, 311.
[3] Al-Baraka and Mohamed, supra note 5, 279.
[4] Adel and Bouchra, supra note 4, 24.
[5] Thunayyan N. Al-Thunayyan, supra note 3, 16.
[6] Shahira and Issa, supra note 2, 305.

devices to prove the non-manipulation of data from the moment the crime occurred until its presentation to the judiciary, which grants the evidence the character of judicial certainty.[1]

The probative value of digital evidence is not limited to cybercrimes only, but extends to include traditional crimes in which technology is used as an auxiliary tool, such as forgery or financial fraud crimes. Criminal jurisprudence acknowledges that digital evidence is the "King of Evidence" in the current era, due to its ability to provide precise and chronologically documented details that oral evidence or human testimony cannot provide with the same accuracy.[2]

The probative value of this evidence in contemporary legal systems is based on technical acceptance before legal acceptance. The court relies on technical reports issued by digital forensic laboratories to form its conviction. Nevertheless, digital evidence remains subject to the principle of "adversarial debate," where it must be presented to the opponents so they can refute or challenge its validity, ensuring a balance of justice between technology and law.[3]

Digital evidence faces a challenge of "credibility" in the face of traditional systems, as it raises doubt in the non-specialist judge regarding the possibility of fabricating images or texts. To enhance this value, the legislator necessitated the availability of "Technical Certainty," which proves that the digital outputs are an identical copy of the original stored in the device, thereby denying any suspicion of tampering or alteration.[4]

Subsection One: Digital Evidence Under the Principle of the Judge's Free Conviction (Free Proof System)

The principle of free conviction is considered a cornerstone in Latin criminal systems, granting the judge broad freedom in accepting any evidence presented before them as long as it has been debated in the session. In this context, the judge finds no legal embarrassment in accepting digital evidence as an evidentiary tool, as they are not restricted by a specific list of evidence, but the criterion is the extent to which their conscience is reassured of the validity of the incident attributed to the accused through this evidence.[5]

In the Free Proof system, digital evidence is equal to other evidence such as witness testimony or physical clues, as the judge possesses the power to estimate its probative value without restriction from the legislator. This system allows the judge to seek the assistance of modern scientific means to uncover the truth, making digital evidence an effective tool in modern criminal justice to overcome the failure of traditional evidence.[6]

Algerian legislation, as a model for the Free Proof system, emphasizes in Article 212 of the Code of Criminal Procedure its right to form its conviction from any evidence leading to the truth. This means that evidence extracted from a computer or the Internet is legally acceptable evidence, and the matter remains confined to the extent of the strength of this evidence in convincing the judge, which is what depends on the experts' report and the clarity of the digital path of the crime.[7]

---

[1]Adel and Bouchra, id. at 52.
[2]Thunayyan N. Al-Thunayyan, supra note 3, 35.
[3]Al-Maamari, supra note 1, 206.
[4]Al-Baraka and Mohamed, supra note 5, 273.
[5]Shahira and Issa, supra note 2, 307.
[6]Al-Maamari, supra note 1, 205.
[7]Adel and Bouchra, supra note 4, 30.

Despite absolute freedom in estimating evidence, the judge in the system of personal conviction is obliged to reason their judgment, i.e., explaining the logical reasons that made them rely on the digital evidence. This conviction must be derived from valid procedures; if it is proven that the digital evidence was obtained by illegal methods, the judge must discard it and not rely on it, in commitment to the principle of legitimacy.[1]

The Free Proof system allows the judge to balance digital evidence and other evidence; they may reject the digital evidence if it contradicts a witness statement or physical clues. This flexibility makes the criminal judge a guardian of the truth and not merely a conduit for texts, as they use reason and technical logic to link digital data to the reality of the committed crime.[2]

Subsection Two: The Challenge of Acceptance Under the Restricted Proof System and the Role of the Technical Expert

The Restricted Proof system (Anglo-Saxon) imposes strict constraints on the acceptance of evidence, where the law pre-determines the acceptable evidence and its legal value. Digital evidence represents a challenge in this system, especially regarding the "Hearsay Rule," where stored data is sometimes viewed as indirect testimony. To bypass this, these systems have developed exceptions allowing the acceptance of computer outputs as original evidence if conditions of stability and credibility are met.[3]

In this system, the role of the technical expert emerges as a decisive element in the acceptance process, where digital evidence is not accepted until after the expert testifies to the validity of the information system that produced it. The expert is the one who provides technical guarantees to the court that the data has not been subject to change, and without this technical testimony, the digital evidence may remain subject to legal exclusion for lacking the "Originality" requirement required in restricted legislations.[4]

The probative value of digital evidence in restricted systems depends on strict technical criteria, such as inventorying evidence and documenting every step of the digital seizure process. Here, the technical expert plays the role of "Translator" who transfers facts from the complex machine language to the clear language of law, allowing the court to estimate the evidence according to the frameworks drawn by the legislator without departing from the list of allowed evidence.[5]

The "Scientific Certainty" provided by the technical expert represents a bridge for the digital evidence to cross to the judicial bench in systems that require conclusive evidence. The challenge lies in convincing the court panel that digital pulses are equivalent in strength to a signed paper document, which is only done through certified digital criminal laboratories that provide technical reports that do not accept doubt from a scientific perspective.[6]

The technical role of experts in proving cybercrime goes beyond mere data extraction to analyzing criminal behavior and matching digital signatures. In the Restricted Proof system, technical expertise is considered the "Leading Evidence," upon which the rest of the

[1]Thunayyan N. Al-Thunayyan, supra note 3, 72.
[2]Al-Baraka and Mohamed, supra note 5, 268.
[3]Shahira and Issa, supra note 2, 300.
[4]Al-Maamari, supra note 1, 204.
[5]Adel and Bouchra, supra note 4, 64.
[6]Thunayyan N. Al-Thunayyan, supra note 3, 38.

legal conclusions are built, necessitating the high-level qualification of experts to ensure that justice **is not lost between the folds of complex information systems.1**

Chapter Two: Technical Procedures for Investigation and Practical Confrontation of Obstacles

This chapter constitutes the core of the procedural process in combating cybercrime, where the research moves from legal theories to practical applications of how to monitor and seize digital evidence. The digital environment imposes on investigative authorities the followance of complex technological paths starting from the moment of inspecting the crime scene and reaching the analysis of data across global networks, with the necessity of keeping pace with the rapid technical development exploited by criminals to hide their traces.

Section One: Adapting Traditional Investigation Procedures to the Digital Environment

The process of adapting traditional procedural measures to the virtual world is considered one of the most delicate issues facing criminal justice, as classical rules were designed to deal with tangible physical matters. With the emergence of cybercrime, investigative authorities realized the necessity of learning how to deal with the computer as a crime scene and how to preserve the evidence it contains, necessitating the employment of technology in extracting evidence in a manner compatible with its intangible nature.[2]

Investigation in cybercrime, or what is known as digital investigation, consists of a set of methods followed to provide information stored in an electronic medium before the judiciary. This requires training investigators and qualifying them to be familiar with the basic techniques of information and communication technologies, to ensure the extraction of digital evidence from a virtual environment and verify its integrity before submitting it as reliable evidence to the court.[3]

Criminal jurisprudence emphasizes that proof in criminal matters is linked to every judicial effort seeking to manifest the truth, and that the information revolution has opened the door to new forms of crimes that cannot be uncovered by traditional means alone. Therefore, adapting procedures means the necessary inclusion of modern means such as surveillance cameras and modern recording devices and tracing digital addresses (IP) as legally recognized investigative tools to link the perpetrator to their digital crime.[4]

Cybercrime requires from search and investigation authorities a special familiarity with computer techniques and information systems, as the lack of expertise in this field constitutes a major obstacle to proving the crime. Hence emerges the challenge in how to adapt the provisions of the code of criminal procedure to include searching information systems and seizing digital data, ensuring that these procedures are carried out within a framework that respects individuals' rights and their fundamental freedoms.[5]

The difficulty of proof in the digital environment dictates that investigators follow precise scientific steps starting from securing the virtual crime scene and preventing any external intervention that may lead to the modification of data. These procedures must be

[1]Seksek Mohamed, supra note 8, 44.
[2]Al-Maamari, supra note 1, 190.
[3]Al-Baraka and Mohamed, supra note 5, 275.
[4]Malika Abudiyar, "Criminal Proof in Cybercrimes," Electronic Journal of Legal Research, no. 2 (2018), 101.
[5]Adel and Bouchra, supra note 4, 59.

technically and legally documented to ensure they are not challenged for their legitimacy, especially since digital evidence is characterized by fragility and ease of erasure, making it completely different from traditional physical evidence.[1]

Subsection One: Digital Inspection and Seizure: Duality of the Crime Scene (Physical and Virtual)

Cybercrime is characterized by the duality of its scene, as it is divided into a physical scene that includes tangible material components such as the device and its accessories, and a virtual digital scene located inside the digital environment and networks. Inspection in the physical scene requires lifting physical fingerprints from the device, while in the virtual scene, it requires dealing with digital data that moves inside the computer or across the Internet by specialists with high technical expertise.[2]

When moving to inspect a cybercrime scene, investigators must start by documenting the state in which the devices, connections, and cables are found, to ensure the ease of subsequent analysis. It is also imperative not to rush into moving any information material before ensuring that the environment is free of any magnetic fields that may lead to the destruction of stored data or their overlapping, reflecting the precise scientific nature of the digital seizure process.[3]

Digital inspection is intended to prove the state in which the crime scene is at the moment of the investigator's arrival, including the digital traces left by the perpetrator. The digital crime scene differs from the traditional one in that it may extend across borders, requiring advanced tracking techniques to discover the "Digital Footprint" that is created without the person's will and constitutes a decisive trace in proving their involvement in the criminal activity.[4]

Seizing evidence in the digital environment is not limited to seizing hard disks, but extends to include all media that may carry data such as "Flash Memory," phone call logs, and even paper documents that may contain passwords. The importance of this duality lies in the fact that physical evidence (the device) is the container that holds the moral digital evidence (the data), and they cannot be separated in the integrated proof process.[5]

Search authorities face the challenge of "evaporating evidence" during inspection, where the perpetrator can destroy the evidence remotely in a few seconds. Therefore, some legislations have allowed the Public Prosecution to expedite inspection procedures and request service providers to track logs and preserve them quickly before a court order is issued, to ensure that digital traces forming the core of the evidence in the virtual world are not lost.[6]

Section Two: Digital Search Techniques: From Physical Components to Information Networks

Digital search is considered one of the most dangerous stages of criminal procedures, as it aims to reach physical or moral evidence that helps in uncovering the truth and

[1]Seksek Mohamed, supra note 8, 35.
[2]Al-Maamari, supra note 1, 210
[3]Thunayyan N. Al-Thunayyan, supra note 3, 59.
[4]Seksek Mohamed, supra note 8, 40.
[5]Adel and Bouchra, supra note 4, 48.
[6]Masoud bin Humaid Al-Maamari, supra note 1, 211.

attributing it to the accused. This search is divided into searching the physical components of the device (Hardware), which is subject to general rules, and searching moral components (data and software), which requires technical skills to extract hidden or encrypted content.[1]

The scope of search in cybercrimes expands to include information networks, where the evidence may be distributed between more than one device or stored in the "Cloud." Investigators face challenges in this regard related to legal entry into systems outside direct physical control, necessitating the use of specialized software to decrypt and trace the path of data across international servers to reach the truth.[2]

When conducting a search of an information system, a written permission from the competent judicial authority must be available, with the necessity of the presence of a specialist in information technology to ensure that no damage is caused to the system. Modern search techniques include intercepting electronic communications and recording sounds and capturing digital images, which are procedures that have been included in criminal procedure laws to face the seriousness of organized crime via the Internet.[3]

Digital search techniques are characterized by the ability to recover deleted or "dead" files, which represents a technological superiority for digital investigation over traditional investigation. If the perpetrator attempts to erase the traces of their crime by deleting files, experts can use advanced software to recover this data from the deep memory of the device, making digital search a comprehensive mining process that does not stop at what is apparent from the data.[4]

The challenge of trans-border search emerges when data is stored in another country, necessitating the activation of international cooperation agreements. In this case, national investigators cannot penetrate those systems without an international judicial delegation, otherwise, the search is considered an assault on the sovereignty of states, except in cases permitted by agreements such as "Expedited Preservation" of data to ensure they are not destroyed before the completion of official procedures to obtain them.[5]

Subsection Two: Overcoming Technical and Procedural Obstacles in Proving Cybercrime

Cybercrime is considered one of the most difficult crimes to prove due to its complex technical nature and the ease of erasing its evidence. To overcome these obstacles, the legislator and the judiciary must transition from concepts of physical proof to concepts of "Scientific Proof," where reliance is placed on digital analysis and matching digital logs (Log Files) as a technical alternative to traditional fingerprints.[6]

Among the most prominent obstacles facing investigation is the criminals' use of "Anti-Digital Forensics" techniques such as strong encryption and identity hiding. Overcoming this requires investigative authorities to employ specialized experts capable of decryption and using "Reverse Engineering" techniques to track criminal behavior, which imposes a major financial and technical burden on security agencies.[7]

---

[1]Al-Maamari, supra note 1, 216.
[2]Thunayyan N. Al-Thunayyan, supra note 3, 65.
[3]Adel and Bouchra, supra note 4, 37.
[4]Al-Baraka and Mohamed, supra note 5, 271.
[5]Seksek Mohamed, supra note 8, 38.
[6]Shahira and Issa, supra note 2, 311.
[7]Thunayyan N. Al-Thunayyan, supra note 3, 123.

The fragility of digital evidence and its rapid disappearance dictate the necessity of developing procedures for "Immediate Preservation," where the digital state of the device or site is frozen immediately upon receipt of a report. This measure helps prevent the loss of volatile data in the Random Access Memory (RAM) that disappears as soon as the device is turned off, which is a fundamental step in ensuring the integrity of the evidence and its subsequent acceptance before the court.[1]

The issue of "Procedural Legitimacy" is another obstacle, as a simple error in the method of extracting data may lead to the nullification of the entire evidence. To bypass this, unified technical and legal protocols must be established that investigators adhere to, ensuring a "Chain of Custody" for the digital evidence from the moment of its seizure until its presentation to the court, to guarantee its credibility and non-exposure to tampering.[2]

The lack of digital culture among some judges represents an obstacle to estimating the value of digital evidence correctly. Facing this obstacle requires intensifying training courses for judges and members of the prosecution, to enable them to discuss the experts' technical reports with a deep understanding, ensuring that the judge's personal conviction is built on solid scientific foundations and not just general impressions.[3]

Subsection One: Obstacles of Rapid Evidence Vanishing and Anti-Forensics Techniques

Digital evidence is characterized by the feature of "Automatic Vanishing," as many digital operations are recorded in temporary memory and erased immediately, or the perpetrator may use programs that wipe activity logs (Cleaning Tools) upon exiting the system. This rapid disappearance imposes on investigators the necessity of "Expedited Bit-stream Imaging" to preserve the state of the data as it is.[4]

Complex encryption techniques (Encryption) represent the greatest challenge to digital investigation, where data becomes unreadable even after being physically seized. Investigators resort to bypassing this obstacle by attempting to obtain passwords through investigation with suspects or using decryption programs, but in many cases, the evidence remains imprisoned behind strong encryption walls, stalling the course of justice.[5]

Professional criminal groups use "Steganography" techniques inside innocent files, such as hiding a criminal text inside an image or video file. This type of camouflage requires the digital expert to have superior analytical skills to detect the presence of abnormal data inside seized files, reflecting the continuous conflict between crime techniques and combat techniques.[6]

The use of self-destructing malware by culprits leads to the erasure of evidence as soon as an attempt to examine the system is detected. This offensive technique imposes on investigation teams the use of isolated environments (Sandboxing) to examine seized devices

[1]Adel and Bouchra, supra note 4, 63.
[2]Seksek Mohamed, id. at 51.
[3]Al-Baraka and Mohamed, supra note 5, 276.
[4]Thunayyan N. Al-Thunayyan, supra note 3, 118.
[5]Al-Maamari, supra note 1, 214.
[6]Seksek Mohamed, supra note 8, 21.

and software, to ensure that automatic erasure commands that the perpetrator may have embedded in the code of the used software are not activated.[1]

Digital proof also faces the "Time-Stamping" problem of files, where the perpetrator can tamper with the dates and times of file creation or modification to provide an alibi. Overcoming this obstacle requires examining deep system logs and comparing them with service provider and network logs to detect any conflict in temporal data, and to ensure the accuracy of the procedural sequence of events.[2]

Subsection Two: Obstacles of Judicial Jurisdiction and the Necessity of International Technical Cooperation

The problem of conflict of judicial jurisdiction is considered one of the most complex obstacles in proving cybercrime, as cyberspace does not recognize geographical borders. The criminal act may start in one continent and end in another, which raises questions about the applicable law and the competent court, necessitating reconciliation between the sovereignty of states and the requirements of pursuing international criminals.[3]

Legal jurisprudence emphasizes that the absence of a unified international policy to cooperate leads to a counter-cooperation and professionalism among "Information Hackers," increasing the effectiveness of their attacks. Therefore, it has become imperative for states to conclude bilateral and collective agreements that guarantee the exchange of digital information and the extradition of criminals, to ensure that national borders do not turn into safe havens for perpetrators of these crimes.[4]

The "Budapest Convention" on Cybercrime is considered an important international reference for technical and cross-border legal cooperation, as it laid down important foundations for "International Judicial Assistance." This assistance allows investigative authorities in one country to request help from the authorities of another country to seize digital evidence stored on its territory, which reduces the gap of spatial jurisdiction.[5]

The importance of international organizations such as "Interpol" emerges in facilitating access to digital addresses of users via fast and secure communication channels. This cooperation helps in shortening the time necessary to determine the identity of perpetrators, especially in cases that require an immediate digital monitoring of data before it is wiped or moved to other information systems in countries that do not cooperate judicially effectively.[6]

International cooperation faces an obstacle manifested in the difference in legal systems (Free Proof vs. Restricted Proof), as some countries may refuse to provide assistance if the act is not a crime in their national law. To overcome this, international recommendations call for the necessity of unifying the minimum legal standards for cybercrimes, to ensure the flow of technical and judicial procedures in the face of global crime.[7]

Conclusion:

[1]Adel and Bouchra, supra note 4, 21.
[2]Al-Baraka and Mohamed, supra note 5, 273.
[3]Adel and Bouchra, supra note 4, 60.
[4]Al-Baraka and Mohamed, id. at 278.
[5]Seksek Mohamed, supra note 8, 55.
[6]Malika Abudiyar, supra note 33, 120.
[7]Shahira and Issa, supra note 2, 313.

The study has revealed that cybercrime represents an exceptional challenge to the criminal system due to its virtual nature that transcends traditional concepts of time and space. The research concluded that proof in these crimes does not rely on tangible physical traces, but rather on interrogating digital pulses and stored data characterized by fragility and ease of erasure, necessitating a radical shift in procedural rules.

Furthermore, the study demonstrated that adapting classical procedural rules to the digital environment required a new understanding of the crime scene, which has become dual, combining the physical entity of the device and the virtual cyberspace. Success in the evidentiary process has become dependent on speed and accuracy in dealing with volatile data, and ensuring a "Chain of Custody" for the digital evidence from the moment of seizure until its presentation to the judiciary to form its certain conviction.

Results:

Among the most important results reached by the research is that digital evidence is a unique type of traditional evidence; it is not purely physical or oral evidence, but rather "Scientific Evidence" stored in a binary non-organized form. Its probative value depends entirely on the integrity of the technical procedures followed in its extraction, making it subject to a standard of technical legality before legal legality.

The results also proved that cross-border search and conflict of judicial jurisdiction represent the greatest obstacle to achieving swift justice in global cyberspace. Information globalization allows perpetrators to hide behind distant international servers, making digital evidence an idle tool in the absence of technical compatibility and effective international judicial cooperation between countries to pursue perpetrators of these crimes.

Recommendations:

The research recommends the necessity of updating national legislations to include explicit texts regulating "Expedited Preservation" procedures for information data and recognizing the validity of electronic signatures as conclusive evidentiary evidence. It is also necessary to establish specialized technical departments in combating cybercrime within security agencies, and providing them with the latest digital laboratories to ensure the seizure of evidence before its technological disappearance.

The recommendations emphasize the inevitability of activating international cooperation through "Interpol" channels and facilitating international delegation procedures to seize digital evidence stored abroad. In addition to the necessity of intensifying specialized training for judges in the fields of digital technology, to enable them to estimate experts' reports and balance them with the rest of the criminal evidence in a scientific manner that guarantees the achievement of justice.

List of References:

1. Thunayyan Nasser Al-Thunayyan, *Proving Cybercrime: A Theoretical and Applied Study*, Master's Thesis, Naif Arab University for Security Sciences, Saudi Arabia, 2012/2013, p. 22.
2. Seksek Mohamed, *Criminal Proof in Cybercrimes*, Master's Thesis, University of Djelfa, 2021/2022, p. 14.
3. Al-Tayeb Al-Baraka and Hadj Soudi Mohamed, *The Problem of Proof in Cybercrimes*, Afaq Ilmiya Journal, Vol. 11, No. 01, 2019, p. 269.

4. Labiad Adel and Nezli Bouchra, *Proving Cybercrime*, Master's Thesis, University of Ouargla, 2017/2018, p. 29.
5. Merghad Shahira and Haddad Issa, *The Probative Value of Digital Evidence Before the Criminal Judiciary*, Journal of the Department of Legal and Political Research and Studies, Vol. 07, No. 02, 2023, p. 297.
6. Masoud bin Humaid Al-Maamari, *Digital Evidence for Proving Cybercrime*, Kuwait International Law School Journal, Special Supplement, No. 3, 2018, p. 193.
7. Malika Abudiyar, *Criminal Proof in Cybercrimes*, Electronic Journal of Legal Research, No. 2, 2018, p. 101.

- **How to cite this article by the APA method:**

BOUDJELLAL Abdelkader, BERRADI Ahmed, **Digital Evidence Engineering: Towards an Integrated Legal and Technical Vision for Proof in the Virtual Environment**, Journal of Politic and Law, Volume ..(number ..), Algeria :KasdiMerbah University Ouargla, pp. .. - …