Proving Electronic Crime With Digital Evidence According to Algerian Legislation

إثبات الجريمة الإلكترونية بالدليل الرقمي وفق التشريع الجزائري

Bourtal Amina
Faculty of Law - University of Ain Temouchent
amina.bourtal@univ-temouchent.edu.dz

Date of submission19/12/2023 /Date of final acceptance:25/03/2024 /Date of publication :mars 2024

Abstract:

Due to technological development and the information revolution, electronic crimes have been committed as a result of the misuse of technology and electronic communication means. The Algerian legislator has organized provisions for the prevention of these emerging crimes, especially by criminalizing attacks targeting automated data processing systems in Law 09-04, which includes special rules for the prevention and combat of crimes related to information technology and communication, as well as laws that address the punitive and criminal aspects. However, in this research, we focused on the uniqueness of electronic crime as being difficult to prove, The perpetrator may escape punishment unless convicted based on convincing digital evidence, according to the free proof system established by the Algerian legislator. This system adopts various modern methods for detecting electronic crime, with the possibility of using some traditional methods when suitable for this modern, transnational type of crime.

Keywords: Crime; Electronic; Evidence; Digital; Proof.

ملخص:

ترتّب عن التطّور التكنولوجي وثورة المعلوماتيّة، ارتكاب جرائم الكترونية، نتيجة سوء استغلال التّكنولوجيا ووسائل الاتّصال الالكترونية، حيث نظم المشرع الجزائري أحكام الوقاية من هذه الجرائم المستحدثة لاسيّما بتجريم الاعتداءات الّتي تستهدف أنظمة المعالجة الآلية للمعطيات في القانون 09-04 المتضمن القواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيا الاعلام والاتصال ومكافحتها، وقوانين تناولت الجانب العقابي والجزائي. غير أنّنا ركزنا في هذا البحث على خصوصية الجريمة الإلكترونية في كونها صعبة الإثبات، فقد يفلت الجاني من العقاب ما لم يُدان بدليل رقمي ذي حجية ثبوتية يقتنع بها القاضي، وفق نظام الإثبات الحرّ الذي أقره المشرع الجزائري باعتماد مختلف الطرق الحديثة للكشف عن الجريمة الالكترونية، مع جواز اعتماد بعض الطرق التقليدية متى تناسبت مع هذا النمط الإجرامي الحديث العابر للحدود.

Auteur correspondant: Bourtal Amina

Introduction

The digital transformation and rapid development in the field of information and communication technologies and the Internet have significantly impacted the commission of electronic crimes. These crimes affect the privacy of individuals and the security of their data, resulting from the evolution of criminal thought. Such crimes, with their unique nature, are now committed using the latest scientific means, which must be criminally proven by uncovering digital evidence. This necessity arises from the widespread use of digital information technologies to identify the perpetrators of electronic crimes, who leave personal data merely by using information and communication technology methods on devices with digital memory capacity.

However, questions arise about the acceptance of this digital evidence in proving electronic crimes and its evidentiary value in front of the criminal judge and their conviction by it. This is especially pertinent after adopting the principle of free proof, recognized by comparative criminal systems, aiming to break away from certain restrictions and enabling the acquisition of evidence derived from the virtual environment through various means of proof. This approach acknowledges the legal validity and evidentiary value of such evidence, influencing the Algerian legislator, who emphasized the admissibility of proving crimes by any means of proof according to the provisions of the amended and supplemented Code of Criminal Procedure.[1]

In the quest to uncover digital evidence and limit attacks on automated data processing systems, the Algerian legislator in Law No. 04-15 dated November 10, 2004, amended and supplemented by Order 66-156 containing the Penal Code,[2] and Law 09-04 dated August 5, 2009, containing special rules for the prevention and combat of crimes related to information technology and communication,[3] authorized monitoring electronic communications and imposed procedural rules related to search, seizure, and defining the obligations of electronic communication operators in preserving data that aids in uncovering these emerging crimes.

However, do these rules suffice to meet the challenges faced by specialized agencies in uncovering digital evidence to prove electronic crimes with their transnational nature, considering the lack of international standardization regarding evidentiary requirements in court? What is the evidentiary strength of digital evidence?

To address these questions raised by the topic under study, we will rely on descriptive and analytical methods, encompassing the most important legal aspects of this topic within two main axesm :

I - The Conceptual Framework of Electronic Crime

II - Digital Evidence and Its Evidentiary Value in Proving Electronic Crime

I - The Conceptual Framework of Electronic Crime

We attempt to define the concept of electronic crime and the extent of the Algerian legislator's interest in regulating its provisions, which are based on elements similar to traditional crimes, as we will discuss below:

A) Concept of Electronic Crime

Electronic crime is a newly emerged crime committed in a virtual environment, and it takes various forms that distinguish it from traditional crimes:

1 - Definition of Electronic Crime

Electronic Crime in Terminology and Legislation define as:

- **Definition of Electronic Crime in Terminology**

Electronic crime represents an assault on a legally protected interest, necessitating the imposition of sanctions to limit its spread within societies. However, technological developments have spawned a new or technical form of criminality,[4] resulting in several information-related crimes that affect both natural and legal persons, public or private,[5] These crimes are committed in a digital environment using a computer and the internet, and exceptional technical capabilities with the aim of making profits or competing for position.[6]

These new crimes are referred to as electronic crimes, computer or internet crimes,[7] which are also known as cybercrimes, information technology crimes,[8] informational embezzlement, informational fraud, due to their special nature associated with computers, distinguishing them from traditional crimes.[9] They involve illegal, unethical, or unauthorized behavior related to the automated processing or transfer of data,[10] committed against computers or other information and communication technology systems with the intent of destruction, damage, or disruption, or using a computer to infiltrate information systems[11] during the automated processing of data and information related to computers, at the stages of data entry, processing, or output.[12]

- **Definition of Electronic Crime in Legislation**

The Organisation for Economic Co-operation and Development (OECD)[13] defines information crime as any act or omission that assaults material and moral assets, directly or indirectly resulting from information technology intervention. Its material existence is only realized by coupling the criminal behavior focused on an information system with the intent to commit unlawful acts, linking this quiet crime with the personality of the criminal,[14] a specialist in computer and internet technologies,[15] who acts as a hacker or professional with high informational intelligence[16] and social adaptability, increasing their criminal danger.[17]

From this perspective, domestic legislations have focused on the necessity of establishing provisions applicable to information systems, including the Algerian legislator who criminalized assaults targeting automated data processing systems under Section 7 bis of Law No. 04-15 dated November 10, 2004, amended and supplemented to the Penal Code under the title "Assault on Automated Data Processing Systems." The legislator emphasized the need to provide legal protection to information systems by imposing sanctions, considering information crime as any crime affecting automated systems, and criminalizing behaviors with negative impact that constitute an assault on the information system.[18]

Electronic crime, according to the provisions of Article 2 of Law No. 09/04 dated August 26, 2009, containing special rules for the prevention of these crimes, includes crimes related to information technology and communication that affect automated data processing systems specified in the Penal Code, and any other crime committed or facilitated through an information system and electronic communication system.

It is evident that the Algerian legislator explicitly omitted a precise definition of electronic crime, leaving this matter to jurisprudence, but expanded the scope of crimes affecting electronic information and communication systems, commonly referred to as crimes related to information technology and communication, imposing penalties provided in the Algerian Penal Code.

2 - Forms of Electronic Crime

The newly emerged crime takes several forms, summarized as follows:

- **Information System Breach Crime**

An automated processing system is a complex consisting of one or more processing units comprising memory, programs, input and output devices, and linking devices, aimed at the automated technical processing of data using new scientific and technical innovations that legislations aim to protect from breach.[19]

- **Computer-Related Crime Computer**

Crimes are linked to the virtual environment except in terms of the means, which are represented in the computer and the internet as auxiliary means for committing the crime. The assault occurs on their physical or moral entity[20] by breaching programs and data stored and exchanged between computers and networks, manipulated either by entering false information or destroying stored information through erasure, modification, or interference with the information system, resulting in the disruption of the computer's automated system[21] to the extent of affecting personal data of individuals.

In this regard, the Algerian legislator enacted Law No. 18-07 dated June 10, 2018, relating to the protection of natural persons in the field of personal data processing.[22] Examples of these crimes include unauthorized electronic transfer of funds using online payment cards.

B) Elements of Electronic Crime

The establishment of electronic crime depends on the necessity of having a legal element,[23] a material element, and a moral element, as we will present below:

1 - Material Element

The material element of electronic crime is represented in the criminal behavior, the criminal result, and the causal relationship, even though the crime can occur without the realization of the result, as the perpetrator is reported before the result occurs. The material element takes several forms, the most important of which are:

- **Information Forgery Crime**

The material element is represented in altering the truth in an official or ordinary document that falls under electronic evidence, such as electronic documents and recordings.[24] In this type of electronic crime, the Algerian legislator referred to the application of the general provisions of forgery in the Algerian Penal Code from Article 214 to Article 229.

- **Assault on Automated Processing Systems Crime**

The material element in the crime of assaulting automated processing systems occurs when illegally entering data processing systems, where the crime occurs without the result being realized, and mere unlawful access is sufficient. In contrast, if the perpetrator commits unlawful behaviors upon entry, deleting or altering the system's data and sabotaging it, the Algerian legislator criminalized acts affecting the automated processing system, and informational fraud, under Section 7 bis of the Penal Code, Article 394 bis, imposing imprisonment from three (3) months to one year and a fine from 50,000 DZD to 100,000 DZD on anyone who enters or remains by fraud in all or part of an automated processing system or attempts to do so, with the penalty being doubled if it results in the deletion or alteration of the system's data. The penalty of imprisonment from six (6) months to two (2) years and a fine from 50,000 DZD to 150,000 DZD is applied.

The Algerian legislator also intensified the penalties under the provisions of Article 394 bis 2 of the Penal Code for the perpetrator who deliberately assaults data, imposing imprisonment from two (2) months to three (3) years and a fine from 100,000 DZD to 500,000 DZD on anyone who deliberately or fraudulently designs, searches, compiles, provides, publishes, trades in stored or processed data or data transmitted through an information system, which can be used to commit the crimes stipulated in this section, possession, disclosure, publication, and use for any purpose of all data obtained from one of the crimes stipulated in this section.

2 - Moral Element

The electronic criminal commits their criminal behavior knowing and directing their will towards realizing the criminal behavior and perceiving matters in a manner corresponding to reality, meaning the presence of a general or specific primary criminal intent is necessary to determine criminal responsibility, proportionate to the nature and type of electronic crime, and the perpetrator's intent to cause harm. Some electronic crimes require a specific intent, such as crimes of defamation on the internet, and the spread of viruses through the network, where the criminal aims to sabotage the network's operation,[25] and the judge has discretionary authority.

II - Digital Evidence and Its Evidentiary Value in Proving Electronic Crime

Electronic crimes are proven with digital evidence, similar to traditional crimes, raising questions about their evidentiary value in criminal proceedings:

A) Concept of Digital Evidence

Digital evidence, in its various forms, possesses unique characteristics that distinguish it from other ordinary scientific evidence. We will explore these aspects below:

1 - Definition of Digital Evidence

Digital evidence, as a modern means in the criminal proof of electronic crimes against natural or legal persons,[26] is cross-border in nature and rapidly transmits from one place to another through communication networks. It belongs to the realm of computer space, where its external, visible traces can be hidden, destroyed, or altered.

Digital evidence is defined as that which relies on electronic technology to prove electronic crimes. It is derived from computer devices, communication networks, and their accessories, in the form of fields or electrical or magnetic pulses, or computational information or data that can be compiled and analyzed using information technology programs. This evidence can be presented in any stage of the investigation or trial to prove the act, object, or person related to the crime, after capturing all information about the perpetrator and recording their movements and behaviors.[27] This allows the criminal judge to form a personal conviction for acquitting or convicting the accused.[28]

From this perspective, digital evidence is a fact from which the judge derives proof and evidence to establish their conviction about a person before the court, unlike scientific evidence, which revolves around assessing material or personal elements, as a legal situation of conclusive evidentiary value that arises from the scientific examination of a material trace left by the crime.[29]

2 - Characteristics of Digital Evidence

Digital evidence, comprising intangible electronic information and data stored in a virtual, immaterial environment, requires computerized tools or software systems related to computers.[30] It is considered a type of scientific technical evidence derived from machines,[31] allowing for the extraction of original copies with scientific and evidentiary value. Unlike traditional criminal

evidence, which can be perceived by the senses, digital evidence can be transformed from intangible to tangible, like extracting and printing information and data from computers.[32]

Digital evidence allows for the retrieval and repair of related data and information after deletion or damage, and for displaying it in the machine's memory after hiding it, making it difficult to completely eliminate.[33] Any attempt by the perpetrator to erase it is recorded in the device's memory as evidence against them.[34] This characteristic is one of the most important aspects of digital evidence compared to ordinary evidence, as there are many computer programs designed to recover deleted or reformatted data.[35]

3 - Types of Digital Evidence

Given the special nature of digital evidence, it takes various forms, unlike other criminal evidence that belongs to a traditional environment.[36] Among the most important types of digital evidence used to present information and prove electronic crimes committed by criminals causing an increase in crime rates are certain types of records created automatically by machines without human intervention and other records preserved only by input. We summarize these types of digital evidence below:

- **Digital Images**

Digital images, as an alternative technology to traditional photographic images, represent visible facts about the crime and are usually presented in paper form or displayed using a screen. The images are captured using remote cameras to monitor and photograph individuals. It has become easy to reduce the size of cameras for periodic image capture, and there are various methods of photography, including video cameras.

- **Audio Recordings**

Judicial police officers are obliged to make recordings as part of criminal evidence, where recordings are captured and stored digitally, including voice conversations on the internet and telephone, using recording devices to capture sound on tapes that can be played back, transferring sound waves from their sources with their individual tones and characteristics, as well as devices that store electrical signals representing sound.

- **Written Texts**

Written texts refer to those typed using digital devices like emails, mobile phones, etc .[37]

- **Records**

Automatically created in electronic devices as digital evidence, without the intention of the computer or network user, these records are relied upon by judges to uncover the truth. Often, the perpetrator leaves an electronic fingerprint of records or data that automatically record and preserve themselves when sending or receiving messages or calls using technical devices and programs, such as surveillance and wiretapping devices to capture wired and wireless conversations and calls made over the internet, phone records, etc.[38]

Digital evidence includes anything that indicates a crime attributed to a person, like someone sending an email containing viruses that damage the recipient's website. This email serves as evidence of the crime and its attribution to a specific person, provided that information confirming their identity is available.

4 - Methods of Uncovering Digital Evidence for Proving Electronic Crime

It is known that electronic crimes are difficult to track and uncover due to the lack of physical traces, being merely changing numbers without material evidence, unlike traditional crimes.[39] However, there are methods and techniques for their detection:

- **Search**

Searching is a procedural method aimed at detecting digital evidence related to electronic crimes, within or outside the country through network connections.[40] It applies to data processing systems and computer memory to search for illegal acts and behaviors[41] by the competent authority. While searching does not align with the immaterial nature of digital criminal evidence, all formal and substantive conditions for conducting electronic searches must be observed.[42]

The Budapest Convention, signed on November 23, 2001,[43] emphasizes the necessity to issue orders for presenting specific data, searching and seizing the content of data stored and transmitted via communication devices, in the computer information system or data storage media, after the intervention of service providers and competent authorities, to ascertain their illegitimate use.

Search may represent one of the investigative procedures carried out by the competent judicial authority and judicial police officers under an order to lawfully enter, even remotely, an information system or part of it, as well as the stored information data, according to Article 5 of Law No. 09-04 dated August 5, 2009, containing special rules for the prevention of crimes related to information technology and communication.

After legitimately collecting digital evidence related to electronic crime with judicial permission,[44] it is explored in programs or data files and data storage and preservation media, such as discs, tapes, computer outputs, and contents stored in the central unit of the system.[45] It is seized by emptying or copying it onto electronic storage media, subject to seizure or placement according to Article 6 of the same law.

- **Inspection**

Inspection, fundamental to criminal investigation, reflects the perpetrator's actions. It is crucial in electronic crimes, capturing evidence that aids in proving their occurrence and attributing them to the perpetrator.[46] The investigator is obliged to inspect the electronic crime within the cyber space using specialized technical skills, avoiding obstacles that hinder the crime's inspection, which involves electromagnetic pulses, to gather information after examining all stored documents and correspondence of the perpetrator, verifying the date of various connections (IP) and tracing their tracks.[47]

- **Expertise**

Electronic crime, as a type that urgently requires technical expertise, is beyond the capability of ordinary experts.[48] Thus, the judge resorts to electronic experts, who must have technical and scientific knowledge according to Article 143 of the Criminal Procedure Code,[49] to extract evidence and clarify ambiguities in the investigated crime and address technical issues presented to them.

- **Testimony**

Testimony is one of the fundamental evidence for proving electronic crimes. The informational or electronic witness must possess expertise in the technical and artistic field to provide understandable testimony to the judge, consistent with the facts of the case.

This includes computer operators with the full capacity to operate electronic devices and their accessories, introducing and transferring information to and from the device according to technical and artistic standards,[50] as well as analysts responsible for collecting and analyzing data and tracking information within electronic systems to locate the processing sites via computer, and maintenance engineers responsible for maintenance works related to computers, their accessories, and related communication networks.[51]

Also, the communication network monitor uses electronic technology to collect data and information about the suspect, aiming to obtain evidence contributing to uncovering the truth and confirming electronic prosecution evidence.[52]

- **Electronic Communications Monitoring**

Similar to some comparative legislations, the Algerian legislator does not require any device for electronic monitoring in Law No. 09-04, containing special rules for the prevention and combat of crimes related to information and communication technologies.

However, resorting to electronic monitoring is restricted to prior written and reasoned permission to conduct the monitoring in crimes affecting the provisions of this law from the competent judicial authorities, represented by the Public Prosecutor at the Algiers Court of Appeal, unlike the general provisions stipulated in the Algerian Criminal Procedure Code, which required permission for electronic monitoring by the Public Prosecutor during the preliminary investigation stage or by the investigating judge during the judicial investigation stage, otherwise the procedure is null according to Article 65 bis 5 of Law No. 66-155 of the Criminal Procedure Code.

B) The Evidential Weight of Digital Evidence in Criminal Proof

The role of criminal evidence in modern criminal policy, particularly in the context of cybercrime, is fundamentally focused on individualizing criminal penalties based on the specific role and character of the accused, whether as a perpetrator or an accomplice.[53] Understanding the admissibility and weight of digital evidence in proving cybercrime is crucial in this context:

1 - The Judicial Authority's Assessment of the Evidential Value of Digital Evidence

The extent of a criminal judge's authority in assessing digital evidence varies from country to country, according to known systems of evidence:

- **Restricted Evidence System**

Considered one of the oldest systems of criminal evidence, where the judge is bound in his decision of acquittal or conviction by the evidence specified by the law, without applying his personal conviction of the evidence's accuracy. As this system does not embrace the principle of judicial conviction, it results in the legislator's conviction replacing that of the judge's.[54]

Under the restricted evidence system, the criminal judge is placed in a rigid framework where legal certainty is based on the presumption of the evidence's accuracy, regardless of the reality or differing circumstances of the case.

However, this involvement of the legislator in matters beyond his purview arises; the acceptance of evidence derived from computers depends on a reasonable cause to believe that such evidence is inaccurate, that the data is unsound, that the computer is malfunctioning, or that it was used without prior permission.[55]

Digital evidence is deemed invalid if obtained in a manner contrary to the law for the purpose of convicting the accused, meaning its acceptance is conditional on being true without any physical

or psychological coercion, as the procedures for collecting digital criminal evidence may conflict with individual freedoms.[56]

- **Free Evidence System**

This system is based on the personal conviction of the criminal judge, who has discretionary power to accept or reject evidence. The judge utilizes various technical methods to prove electronic crimes,[57] exerting effort to reveal the truth after gathering all elements of the incident, investigating, and relying on experts,[58] aiming to arrive at a complete truth without any doubt. The judge is compelled to accept evidence of electronic crimes.

However, the judge's freedom in conviction is not absolute; personal assumptions or speculations must not replace evidence. Instead, the judge must follow the evidence and avoid personal perceptions, ensuring that his reasoning is governed by logic and that the evidence leads to a logical conclusion. The evidence must be legitimate so that the judge does not give free rein to his subjective views and allows for its discussion by the parties involved, without any ambiguity or confusion. These conditions are intended to limit the judge's freedom.[59]

The assessment of digital evidence extracted from electronic media is subject to the competent court's jurisdiction, which is obliged to examine it in a court session to discuss it in the presence of the parties involved in the electronic crime. This process aims to reach a truth that satisfies the judge's conscience, who enjoys discretionary power in evaluating digital evidence,[60] which holds evidential value in proving electronic crimes, after referring to a technical expert's opinion.

The evidence is subject to the judge's discretionary power, who is convinced of it definitively. The inferences drawn are based on scientific and mathematical rules that leave no room for doubt or interpretation, provided they are related to the incident and consistent with the logical sequence of events. However, this does not extend to technical issues; they cannot be debunked except by technical evidence subject to the absolute discretion of the trial court through another technical expertise.[61]

Some jurists believe that digital evidence, to hold evidential value in criminal proof, must be extracted electronically through legitimate means and based on certainty. It is essential to discuss it in a court session in the presence of the parties involved in the electronic crime. The competent judge must arrive at complete certainty with the electronic outputs and the digital evidence generated from them. The judge must perceive these outputs through his senses by observing, examining, analyzing, and deducing to be able to link these outputs to the facts of the case presented to him.[62]

2 - The Algerian Legislator's Stance on the Evidential Value of Digital Evidence:

The Algerian legislator clearly establishes the evidential value of scientific material evidence through its explicit provision for the criminal judge to rely on any evidence deemed necessary to uncover the truth, in line with the principle of free criminal proof.

The digital evidence is deemed valid as long as the judge is convinced of it unequivocally, and it has been extracted lawfully. Article 212/1 of the Algerian Code of Criminal Procedure states, "Crimes may be proven by any means of proof, except in cases where the law specifies otherwise, and the judge may issue his judgment according to his personal conviction..."[63]

This means that the Algerian legislator grants the judge the freedom to base his judgment according to his personal conviction, enabling him to convict the accused based on digital evidence, without being obliged to adhere to a specific type of evidence.

The judge may disregard the evidence if in doubt, provided that the digital evidence is not susceptible to doubt so as not to be interpreted in favor of the accused. However, even if the Algerian legislator allows the judge the freedom to rely on digital evidence related to electronic crimes, it is imperative that this does not infringe on individuals' privacy and freedoms, in accordance with the provisions of Article 47 of the Algerian Constitutional Amendment.[64]

Conclusion:

In concluding this research paper, we deduce that electronic crime has unique characteristics that distinguish it from traditional crime, which is proven by physical evidence. This distinction arises from the evolution of communication and information technology systems and the methods of committing such crimes by electronic criminals, whose identities are difficult to discern except by relying on digital evidence extracted from the virtual environment, aligning with the nature of electronic crime.

Moreover, it cannot be denied that the proof of electronic crimes has received significant attention from the Algerian legislator, akin to other comparative legislations, adopting the free evidence system. This aligns with the nature of electronic crimes, committed through various electronic, technical, and artistic methods, giving the judge discretionary power in their assessment based on personal conviction, as long as it does not violate individuals' freedoms and privacies.
We propose the following recommendations:

- Seek advanced technological methods to identify perpetrators of electronic crimes, reducing obstacles faced by competent authorities.
- Establish legal controls for electronic surveillance as stipulated in the provisions of Law No. 09-04 on the specific rules for preventing crimes related to information and communication technology and combating them, facilitating the extraction of digital evidence to prove electronic crimes.
- Conduct training courses to develop the skills of human resources, particularly experts in investigating electronic crime evidence.
- We encourage Algeria to join and ratify the 2001 International Convention on Combating Internet Crimes, given that the Algerian legislator was influenced by it.
- It is necessary to conclude regional and international agreements to enhance international cooperation in combating electronic crime.

[1] Order No. 66-155 dated June 8, 1966, which includes the amended and supplemented Code of Criminal Procedure, by Law No. 04-14 dated November 10, 2004, Official Journal No. 71, 2004, and Order No. 20-04 dated August 30, 2020, Official Journal No. 51 dated August 31, 2020, and Order No. 21-11 dated August 25, 2021, Official Journal No. 65, dated August 26, 2021.
[2] Law No. 04-15 dated November 10, 2004, which includes the amended and supplemented Penal Code to Order No. 66-156 dated June 8, 1966, Official Journal No. 71, dated November 10, 2004.
[3] Law 09-04 dated August 5, 2009, contains special rules for the prevention and combat of crimes related to information and communication technologies, Official Journal No. 47, issued on August 16, 2009.
[4] Saad Ali Rizk, Implications of the Digital Transformation on Contemporary Criminal Policy, Legal and Economic Studies Journal, Sadat City University, Egypt, Volume 7, Issue 2, December 2021, p. 196.
[5] Adel Youssef Abdel Nabi El-Shokry, Information Crime and the Crisis of Criminal Legitimacy, Kufa Studies Center Journal, Iraq, Issue 7, Year 2008, p. 118.

[6] Ibid., p. 115.
[7] Al-Ajmi Abdullah Daghash, The Practical and Legal Problems of Electronic Crimes : Comparative Study, Magister thesis, specialty of Public law, Faculty of Law, Middle East University Jordan, Year 2014, p. 7-8.
[8] Al-Hajjar Adnan Ibrahim/ Fayez Khader Bashir, Digital Evidence and the Proof of Cyber Crimes: Between Founding and Interpretation, University of Al Istiqlal Journal for Research, Palestine, Volume 6, Issue 1, October 2021, p. 132.
[9] Ibid, p. 136.
[10] Mezaour nassima/ Abdel hamid djedid/ ouled himouda djamaa, electronic crime, IJTIHAD journalon legal and economic studies, university of tamanrasset, volume 10, Issue 1, Year 2021, p 35.
[11] Lotfi Khaled Hassan Ahmed, The Law Applicable to Information Crime, 1st ed, Dar Al-Fikr Al-Jam'i, Egypt, Year 2019, p. 13.
[12] Al-Ajmi Abdullah Daghash, Op. cit., p. 24
[13] It should be noted that the Organisation for Economic Co-operation and Development (OECD) is an economic organization established on September 30, 1961, to address the economic and social challenges posed by globalization. Refer to :
- Reference Definition of OECD's Direct International Investments, Fourth Edition 2008, OECD, p. 2. Published on: www.oecd.org Consulted on 07/09/2023.
[14] Lotfi, Khaled Ahmed Hassan, Op. cit., pp. 31-33.
[15] Al-Hajjar Adnan Ibrahim/ Fayez Khader Bashir, Op. cit., p. 137.
[16] Masri Abdel Sabour Abdel Qawi Ali, The Digital Court and Information Crime (Comparative Study), 1st ed, Law and Economics Library, Riyadh, Year 2012, p. 52.
[17] Ghannam Mohammed Ghannam, The Role of Penal Law in Combating Computer and Internet Crimes and Organized Fraud Using the Internet, Dar Al-Fikr wal-Qanun, Egypt, Year 2010, p. 15.
[18] Salim Maziyoud, Information Crimes: Their Reality in Algeria and Mechanisms of Combat, Algerian Journal of Economics and Development, Yahia Fares University of Médéa, Issue 1, April 2014, p. 104.
[19] Fteeh Raad Fajr/ Yasser Awad, Proving Electronic Crime with Scientific Evidence, Tikrit University Journal for Law Studies, Iraq, volume 1, Issue 2, Year 2017, p. 480.
[20] Al-Hudairi Al-Hassan Al-Tayeb Abdel Salam Al-Asmar, Criminal Evidence Through Modern Scientific Means (A Comparative Study between Libyan Criminal Law and Contemporary Jurisprudence), Magister thesis, specialty sharia and law, Faculty of Graduate School, Maulana Malik Ibrahim State Islamic University Malang, Indonesia, Year 2016, p. 64.
[21] Fteeh Raad Fajr/ Yasser Awad, Op. cit., p. 484.
[22] Law No. 18-07 of June 10, 2018, on the Protection of Natural Persons in the Processing of Personal Data", Official Journal No. 34, dated June 10, 2018.
[23] It's important to note that there can be no crime or punishment without a legal provision. The Algerian legislator has addressed assaults on automated data processing systems, which fall under electronic crime, in Articles 394 bis to 394 bis 7 of Law No. 04-15 dated November 10, 2004, which includes the amended and supplemented Algerian Penal Code, and Article 303 bis 3 of Law No. 06-23 dated December 20, 2006, Official Journal No. 84.
[24] Fteeh Raad Fajr/ Yasser Awad, Op. cit., p. 480.
[25] Ibid, p. 482.
[26] In language, "evidence" is defined as a guide, a collection of proofs or testimonies, or something that leads to a deduction. The term "guide" in this context means to direct or show the way. In technical terms, it refers to that which necessitates knowledge, whereby the mind reaches certain belief in what was previously doubted. Essentially, it is about using evidence to arrive at the truth.
Refer to : Al-Hajjar Adnan Ibrahim/ Fayez Khader Bashir. Op. cit., p. 134.
[27] Fteeh Raad Fajr/ Yasser Awad, Op. cit., pp. 485-487.

[28] Al-Hajawi Ihab Fouad, The Evidential Weight of Digital Evidence in Criminal Proof, Journal of Legal and Economic Sciences, Ain Shams University, Egypt, volume 56, Issue 1, July 2014, pp. 147-148.
[29] It's important to note that scientific physical evidence is one of the types of evidence derived from material elements. This evidence can vary between indirect physical evidence, which does not directly indicate the occurrence of an event but requires deep investigation and rational inference, and direct evidence, which requires specific procedures to utilize and is considered conclusive in its indication, leaving no need for interpretation or explanation. Refer to : Fteeh Raad Fajr/ Yasser Awad ; Op. cit., p. 486.
[30] Al-Hawamdeh Lawrence Said, The Evidential Weight of Digital Evidence in Criminal Proof: A Comparative Analytical Study, Journal of Jurisprudence and Legal Research, Issue 36, October 2021, p. 898.
[31] Al-Hudairi, Al-Hassan Al-Tayeb Abdel Salam Al-Asmar, Op. cit., pp. 58-59.
[32] Al-Hawamdeh Lawrence Said, Op. cit., p. 901.
[33] Fteeh Raad Fajr/ Yasser Awad, Op. cit.,p. 487.
[34] Al-Hudairi, Al-Hassan Al-Tayeb Abdel Salam Al-Asmar, Op. cit., p. 60.
[35] Fteeh, Raad Fajr, and Yasser Awad, Op. cit., p. 487.
[36] Al-Otaibi Ziad Bin Mohammed Aadi, An Exploratory Study on the Evidential Weight of Digital Evidence in Proving Information Crimes, Comprehensive Multidisciplinary Electronic Journal, Jordan, Issue 29, October 2020, p. 13.
[37] Al-Hudairi Al-Hassan Al-Tayeb Abdel Salam Al-Asmar, Op. cit., pp. 62-69.
[38] Al-Hawamdeh Lawrence Said, Op. cit., p. 904.
[39] Masri Abdul Sabour Abdul Qawi Ali, Op. cit., p. 51.
[40] It's important to note that controlling transnational electronic crimes becomes challenging when data records are located in another country. However, an inspection warrant can be issued if a crime occurs in a computer system located within the state. The warrant applies only to this specific computer system. If the computer is connected to another system, the inspection cannot extend to it, even if it contains evidence of a crime, unless a new warrant is issued. This situation necessitates international cooperation for evidence collection. Refer to : Al-Hajawi Ihab Fouad. Op. cit., p. 197.
[41] Laouarim Wahiba, Digital Evidence in the Field of Criminal Proof According to Algerian Legislation, National Criminal Journal, National Center for Social and Criminal Research, Cairo, volume 57, Issue 2, July 2014, p. 90.
[42] It should be noted that among these conditions are the rationale for the search warrant and the type of system to be inspected, while maintaining the confidentiality of the information. Refer to : Abdul Karim Ahmed Sabah, Emerging Crimes due to Technological Development and Their Impact on Criminal Policy, PhD thesis, specialty specialty of Public law, Faculty of Law, University of Karbala, Iraq, Year 2023, p. 179.
[43] The International Convention on Cybercrime, concluded in Budapest on November 23, year 2001.
[44] Ghannam Mohammed Ghannam, Op. cit, p. 192.
[45] Al-Hajawi Ihab Fouad, Op. cit., p. 196.
[46] Masri Abdul Sabour Abdul Qawi Ali, Op. cit., p. 366.
[47] Al-Hajawi, Ihab Fouad. Op. cit., p. 190.
[48] Nassar Ghada, Terrorism and Cybercrime, 1st ed, Al-Arabi, Cairo, Year 2017, p. 36.
[49] The Article 143 of the Code of Criminal Procedure states: "Investigative or judicial authorities, when presented with a matter of a technical nature, may order the appointment of an expert, either upon the request of the Public Prosecution, on their own initiative, or at the request of the parties involved."
[50] Al-Hawamdeh Lawrence Said, Op. cit., p. 919.
[51] Ibid, p.923.

[52] Ben Bada Abdel Halim, Electronic Surveillance as a Measure for Extracting Electronic Evidence: Between the Right to Privacy and the Legitimacy of Electronic Evidence, Academic Journal for Legal Research, Abdel Rahman Mira University of Bejaia, volume 10, Issue 3, Year 2019, p. 394.
[53] Abderrahmane Khalifi, Criminal Procedures in Algerian and Comparative Legislation, 3rd ed., Dar Belkis, Algiers, Year 2017, p. 68.
[54] Ibid, p. 72.
[55] Al-Hajjar Adnan Ibrahim/ Fayez Khader Bashir, Op. cit., p. 144..
[56] Fteeh Raad Fajr/ Yasser Awad. Op. cit., pp. 488-489.
[57] Al-Hashimi Hamza, Proof in Criminal Matters, 2nd ed, Dar Houma, Algiers, Year 2021, p. 7.
[58] Al-Hawari Shaaban Mahmoud Mohamed, Criminal Evidence, 1st ed, Dar Al-Fikr wal Qanoun, Mansoura, Year 2013, p. 27.
[59] Al-Asmar Al-Hudairi Al-Hassan Al-Tayeb Abdel Salam, Op. cit., pp. 32-33.
[60] Al-Hawamdeh, Lawrence Sa'id, Op. cit., p. 925.
[61] Fityeh, Ra'ad Fajr, and Yaser Awad, Op. cit., pp. 488–489.
[62] Al-Hawamdeh, Lawrence Said, Op. cit., p. 925.
[63] Order No. 20-04 of 30 August 2020, amending and supplementing Order No. 66-155 of 8 June 1966 on the Code of Criminal Procedure, Official Gazette No. 51, dated 31 August 2020.
[64] Presidential Decree No. 20-442 of 30 December 2020, concerning the issuance of the constitutional amendment approved in the referendum of 1 November 2020, Official Gazette No. 82, dated 30 December 2020.

Bibliography:

A- Books:

1- Al-Hashimi Hamza, Proof in Criminal Matters, 2nd ed, Dar Houma, Algiers, Year 2021.
2- Al-Hawari Shaaban Mahmoud Mohamed, Criminal Evidence, 1st ed, Dar Al-Fikr wal Qanoun, Mansoura, Year 2013.
3- Abderrahmane Khalifi, Criminal Procedures in Algerian and Comparative Legislation, 3rd ed., Dar Belkis, Algiers, Year 2017.
4- Ghannam Mohammed Ghannam, The Role of Penal Law in Combating Computer and Internet Crimes and Organized Fraud Using the Internet, Dar Al-Fikr wal-Qanun, Egypt, Year 2010.
5- Lotfi Khaled Hassan Ahmed, The Law Applicable to Information Crime, 1st ed, Dar Al-Fikr Al-Jam'i, Egypt, Year 2019.
6- Masri Abdel Sabour Abdel Qawi Ali, The Digital Court and Information Crime (Comparative Study), 1st ed, Law and Economics Library, Riyadh, Year 2012.
7- Nassar Ghada, Terrorism and Cybercrime, 1st ed, Al-Arabi, Cairo, Year 2017.

B – Theses

1- Abdul Karim Ahmed Sabah, Emerging Crimes due to Technological Development and Their Impact on Criminal Policy, PhD thesis, specialty specialty of Public law, Faculty of Law, University of Karbala, Iraq, Year 2023.
2- Al-Hudairi Al-Hassan Al-Tayeb Abdel Salam Al-Asmar, Criminal Evidence Through Modern Scientific Means (A Comparative Study between Libyan Criminal Law and Contemporary Jurisprudence), Magister thesis, specialty sharia and law, Faculty of Graduate School, Maulana Malik Ibrahim State Islamic University Malang, Indonesia, Year 2016.
3- Al-Ajmi Abdullah Daghash, The Practical and Legal Problems of Electronic Crimes : Comparative Study, Magister thesis, specialty of Public law, Faculty of Law, Middle East University Jordan, Year 2014.

C - Journal articles

1- Al-Hawamdeh Lawrence Said, The Evidential Weight of Digital Evidence in Criminal Proof: A Comparative Analytical Study, Journal of Jurisprudence and Legal Research, Issue 36, October 2021.
2- Al-Otaibi Ziad Bin Mohammed Aadi, An Exploratory Study on the Evidential Weight of Digital Evidence in Proving Information Crimes, Comprehensive Multidisciplinary Electronic Journal, Jordan, Issue 29, October 2020.
3- Al-Hajawi Ihab Fouad, The Evidential Weight of Digital Evidence in Criminal Proof, Journal of Legal and Economic Sciences, Ain Shams University, Egypt, volume 56, Issue 1, July 2014.
4- Adel Youssef Abdel Nabi El-Shokry, Information Crime and the Crisis of Criminal Legitimacy, Kufa Studies Center Journal, Iraq, Issue 7, Year 2008.
5- Al-Hajjar Adnan Ibrahim/ Fayez Khader Bashir, Digital Evidence and the Proof of Cyber Crimes: Between Founding and Interpretation, University of Al Istiqlal Journal for Research, Palestine, Volume 6, Issue 1, October 2021.
6- Ben Bada Abdel Halim, Electronic Surveillance as a Measure for Extracting Electronic Evidence: Between the Right to Privacy and the Legitimacy of Electronic Evidence, Academic Journal for Legal Research, Abdel Rahman Mira University of Bejaia, volume 10, Issue 3, Year 2019.
7- Fteeh Raad Fajr/ Yasser Awad, Proving Electronic Crime with Scientific Evidence, Tikrit University Journal for Law Studies, Iraq, volume 1, Issue 2, Year 2017.
8- Laouarim Wahiba, Digital Evidence in the Field of Criminal Proof According to Algerian Legislation, National Criminal Journal, National Center for Social and Criminal Research, Cairo, volume 57, Issue 2, July 2014.
9- Mezaour nassima/ Abdel hamid djedid/ ouled himouda djamaa, electronic crime, IJTIHAD journalon legal and economic studies, university of tamanrasset, volume 10, Issue 1, Year 2021.
10- Salim Maziyoud, Information Crimes: Their Reality in Algeria and Mechanisms of Combat, Algerian Journal of Economics and Development, Yahia Fares University of Médéa, Issue 1, April 2014.
11- Saad Ali Rizk, Implications of the Digital Transformation on Contemporary Criminal Policy, Legal and Economic Studies Journal, Sadat City University, Egypt, Volume 7, Issue 2, December 2021.

D – International Conventions and Legal Texts

- **International Conventions**

- The International Convention on Cybercrime, concluded in Budapest on November 23, year 2001.

- **Legal Texts**

1- Presidential Decree No. 20-442 of 30 December 2020, concerning the issuance of the constitutional amendment approved in the referendum of 1 November 2020, Official Gazette No. 82, dated 30 December 2020.
2- Order No. 66 -155 dated June 8, 1966, which includes the amended and supplemented Code of Criminal Procedure, by Law No. 04-14 dated November 10, 2004, Official Journal No. 71, 2004, and Order No. 20-04 dated August 30, 2020, Official Journal No. 51 dated August 31, 2020, and 3- Order No. 21-11 dated August 25, 2021, Official Journal No. 65, dated August 26, 2021.
3- Law No. 04-15 dated November 10, 2004, which includes the amended and supplemented Penal Code to Order No. 66-156 dated June 8, 1966, Official Journal No. 71, dated November 10, 2004.
4- Law No. 09-04 dated August 5, 2009, contains special rules for the prevention and combat of crimes related to information and communication technologies, Official Journal No. 47, issued on August 16, 2009.

5- Order No. 20-04 of 30 August 2020, amending and supplementing Order No. 66-155 of 8 June 1966 on the Code of Criminal Procedure, Official Gazette No. 51, dated 31 August 2020.
6- Law No. 04-15 dated November 10, 2004, which includes the amended and supplemented Algerian Penal Code.
7- Law No. 06-23 dated December 20, 2006, amending and supplementing Penal Code, Official Journal No. 84.
8- Law No. 18-07 of June 10, 2018, on the Protection of Natural Persons in the Processing of Personal Data, Official Journal No. 34, dated June 10, 2018.

E - Websites

- www.oecd.org
Consulted on 07/09/2023