Pegem Journal of Education and Instruction, Vol. 16, No. 1, 2026 (pp. 622-633)

RESEARCH ARTICLE WWW.PEGEGOG.NET

Modern cybercrimes and the challenges of criminal proof

Dr. Meddah Rima Madjouba

University Center of Aflou, Algeria. Email: m-meddah@cu-aflou.edu.dz

Received : 12/07/2025 ; Accepted : 23/11/2025 ; Published : 11/01/2026

Abstract

In recent Years , the widespread use of digital technologies has led to the emergence of modern cybercrimes, characterized by complexity , speed, and cross -border nature. This situation poses significant challenges for criminal evidence , as traditional Methods are no longer sufficient to prove such crimes. Reliance on digital evidence has become essential, raising legal , technical , and procedural issues related to its collection, preservation , and judicial evaluation , while Ensuring the protection of fundamental rights and freedoms .

This study It aims to examine modern cybercrimes and the challenges of criminals evidence in this context by exploring the conceptual framework of digital crimes, methods of criminal proof, legal and technical challenges, reviewing international experiences and modern approaches , and analyzing the Algerian context to propose policy Recommendations for enhancing the effectiveness of the judicial system in combating These crimes. The research adopts a comparative analytical methodology , combining legal texts review , religious doctrine, and international experiences , to develop an integrated perspective addressing digital evidence challenges and offering practical solutions.

Keywords : Cybercrime - Criminal Evidence - Digital Evidence - Legal Challenges - Criminal Policy - International Experiences

Introduction

has witnessed tremendous advancements in the use of information and communication technologies, leading to an unprecedented ,revolution across various economic, social and cultural spheres. While these transformations have brought significant ,benefits, they have also generated new risks most notably the emergence of sophisticated cybercrimes characterized by continuous evolution, rapid execution, difficulty in tracking, and reliance on diverse digital environments that transcend traditional national borders .

Modern cybercrimes are among the most significant challenges facing criminal justice systems today. Traditional physical evidence ;is no longer sufficient to prove these crimes instead, criminal investigations rely on digital evidence that requires advanced technical skills, knowledge of digital law, and modern forensic analysis tools. This reality raises fundamental issues, most notably how to ,collect digital evidence, ensure its integrity and guarantee its admissibility in court, while safeguarding citizens' fundamental rights and freedoms, especially the right to privacy and the confidentiality of personal data .

Hence, the importance of studying modern cybercrimes and the challenges of criminal proof, as it aims to provide a comprehensive understanding of the legal and technical dimensions of these crimes, review international experiences and modern approaches, analyze the reality of Algeria in this field, and formulate policy and practical recommendations to enhance the effectiveness of the judicial system in the face of digital threats .

,This research includes five main axes beginning with the conceptual framework of cybercrimes, where its concept, characteristics and types are defined, followed by criminal evidence in cybercrimes, which deals with the

means of collecting digital evidence and the criteria for evaluating it, then the technical and legal challenges facing the proof of these crimes, followed by international experiences and modern approaches, and finally the reality of Algeria and policy recommendations to enhance the ability of criminal justice to deal with cybercrimes effectively and efficiently .

The research is based on a comparative analytical methodology between national and international experiences, with reference to legal texts, jurisprudence, and modern scientific studies, in order to provide an integrated vision that clarifies the most prominent difficulties and lays the foundations for developing digital criminal policies in line with global transformations, achieving justice .and ensuring the protection of rights

First axis: The conceptual framework of cybercrimes

Over the past two decades, the world has witnessed tremendous technological transformations, leading to the emergence of a vast and interconnected digital environment that provides unparalleled access to information and services. With this advanced digital environment, cybercrime has emerged as one of the most prominent security and .legal challenges facing modern societies Crimes are no longer limited to traditional physical assaults but are now perpetrated through digital networks and information systems, making it difficult for the traditional judicial system to keep pace using [1].conventional methods of proof

The importance of studying cybercrime stems from its multifaceted nature; it threatens the financial security of individuals and institutions, jeopardizes privacy, targets critical national infrastructure, and causes .widespread moral and economic damage Given this evolution, the urgent need has arisen for a precise scientific definition of cybercrime that ensures a comprehensive ,understanding of its nature, characteristics causes, and various forms, enabling the [2].judicial system to address it effectively

2. Definition of cybercrimes

Cybercrime can be defined as any unlawful act committed using computers or digital networks with the intent to harm information, systems, individuals, or ,institutions, whether the objective is financial Legal definitions vary[3] .moral, or political between countries, but they all agree that these crimes encompass all acts aimed at damaging information systems or illegally exploiting digital resources .

In the international context, the Budapest Convention on Cybercrime (2001) is considered the primary reference for defining cybercrime . It identifies prohibited acts such as unauthorized access to systems, online fraud, and the misuse of personal data, while emphasizing the importance of international .cooperation in combating this type of crime Modern legal scholarship confirms that[4] cybercrime is not simply a replication of traditional online crimes, but rather possesses distinct technical characteristics that differentiate it from other forms of crime .

3. Characteristics of cybercrimes

Cybercrimes are characterized by several features that make them more complex than traditional crimes, most notably :

immaterial nature : The crime can be committed without any physical presence between the perpetrator and the victim, which reduces the possibility of traditional surveillance and makes tracking the trail [5].difficult

: **Speed and widespread reach** Cybercrime can affect thousands of people or organizations within minutes, as happens in ransomware attacks or bank data theft .

International Transit : Many cybercrimes do not adhere to geographical boundaries, as the perpetrator may be in one country and the victim in another, which complicates matters of jurisdiction and [6].international cooperation

Difficulty in : **identifying perpetrators** Cybercriminals rely on anonymity and encryption techniques, in addition to using dark web networks , which makes it more difficult to reach them legally .

:Its reliance on modern technologies Digital crimes exploit the development of

software and smart technologies, including artificial intelligence and digital currencies, to conceal the trace of the crime and expand its .scope

4. Reasons for the emergence of cybercrimes

The emergence of cybercrime is due to a combination of social, technological, and legal factors :

The massive digital expansion : The widespread use of the internet and smart devices has created a fertile environment for committing digital crimes .

Easy access to information : The internet and global networks provide easy ways to access users' data and information, which facilitates fraud and espionage .

: **Weakness of traditional legislation** Many old laws are no longer suitable for dealing with the technical complexities of digital crimes, giving perpetrators more room to operate without effective legal deterrence .

Technological advancements : Modern technologies, such as encryption and digital currencies, have made it easier to commit complex financial crimes that are difficult to . track and investigate

Lack of digital awareness among some individuals and institutions: Weak digital literacy increases the vulnerability of ,individuals and institutions to cybercrimes such as email hacking or digital identity theft .

5. Types of cybercrimes

Cybercrimes vary depending on the nature of the act and its impact, and some of the most prominent include :

:Hacking into systems and databases where the perpetrator gains unauthorized ,access to the systems with the purpose of theft .sabotage, or industrial espionage

Cyber fraud and extortion : This includes phishing , extorting victims with personal information or photos, or financial fraud via electronic payment platforms .

Crimes against privacy : such as spying on individuals, hacking personal accounts, or publishing private photos and data without the victim's consent .

critical **infrastructure** : These crimes target electricity, water, and communications networks, and can lead to serious economic .and national damage

Crimes related to artificial intelligence and digital currencies include exploiting cryptocurrencies for money laundering or using artificial intelligence techniques to develop new fraudulent methods.[11]

6. The legal framework for cybercrimes in Algeria

The Algerian legislator addressed cybercrimes through Law No. 09-04 relating to crimes related to information and communication technology, which defined the types of cybercrimes and their penalties, with a focus on protecting data and information and .ensuring the security of digital networks

However, practical application faces numerous challenges, most notably the limited technical expertise of some judges and judicial police officers, and the difficulty of tracking down perpetrators due to encryption and the ,use of dark web networks. Therefore developing specialized digital investigation units remains a pressing necessity to ensure the effectiveness of the judicial system in .combating cybercrime

axis : Criminal evidence in cybercrimes

1. General Introduction to Digital Forensics

Criminal evidence is the cornerstone of public prosecution, as a defendant cannot be held criminally liable unless their responsibility is proven beyond a reasonable doubt. However, the evolution of cybercrime has brought about a profound shift in the nature of evidence. Criminal evidence is no longer physical or tangible in most cases, but rather digital and intangible, consisting of data, signals, and electronic records that can [7].be altered or destroyed at any moment

In this context, the concept of digital criminal evidence has emerged as a set of legal and technical means that enable judicial authorities to detect cybercrime, identify perpetrators, and attribute criminal acts to them using digital evidence extracted from information systems. This type of evidence is characterized by its requirement for a close integration of law and technology, which presents the criminal judge with a dual

challenge: understanding the technical facts [8].and legally interpreting them

2. The concept of digital evidence and its legal nature

Digital evidence refers to any information of probative value that is created, stored, or transmitted electronically and can be used to establish the occurrence of a crime or attribute it to a specific perpetrator. This includes data stored on computers and smartphones, system logs , emails, application conversations, IP addresses, and data from servers and the [9].cloud

From a legal standpoint, digital evidence raises the issue of its classification within traditional means of proof. Is it considered written evidence? Or technical evidence ? Or an independent type of evidence? Some legal scholars have considered digital evidence as a new type of criminal evidence that requires special regulation, given its fundamental difference from traditional evidence in terms of nature, methods of extraction, and [10].evaluation

This trend confirms that subjecting digital evidence to traditional rules of proof without special adaptation may lead to emptying it of its practical value, or to compromising the guarantees of a fair trial, especially with regard to the rights of the defense and the presumption of innocence .

3. The characteristics of digital evidence and its impact on criminal proof

Digital evidence possesses several characteristics that make it more complex to handle compared to traditional forensic evidence. Firstly , it is intangible; it cannot be perceived by the naked senses and requires technical means for its presentation and analysis. Secondly , it is highly susceptible to alteration, deletion, or copying without leaving a visible trace, which raises serious concerns regarding the integrity and [11].authenticity of the evidence

Furthermore, digital evidence is often distributed across multiple systems and servers that may be located in different countries, complicating its collection and raising issues of jurisdiction and international cooperation. In addition , some digital evidence is encrypted or hidden using advanced technologies, requiring highly specialized technical expertise to decrypt and [12].analyze it

These characteristics directly affect the rules of criminal evidence, as they require a reconsideration of the standards of judicial conviction, and necessitate the development of special mechanisms to verify the reliability of digital evidence before its adoption in conviction .

4. Methods of criminal proof in cybercrimes

The means of criminal proof in cybercrimes are diverse, encompassing a wide range of digital evidence that varies in nature and probative value. Among the most prominent of these are login and connection logs, which reveal the times of access to digital systems, the internet addresses used, and the types of transactions performed. These are considered crucial evidence in linking the perpetrator to the criminal act .

Electronic communications, such as emails and digital chats, are also effective forms of evidence, particularly in fraud and extortion cases, provided they can be verified as belonging to the accused and have not been tampered with. Similarly, data extracted from smartphones, such as photos, messages, and location records, constitutes a significant [13].source of evidence for criminal activity

Furthermore , a technical expert plays a pivotal role in interpreting and analyzing digital evidence, as the court often relies on expert reports to establish the connection between the accused and the digital data in question. Legal scholars generally consider digital expertise a near-mandatory element in this type of case, given the complexity of the .technical issues involved

5. The admissibility of digital evidence in criminal courts

is one of the most contentious issues in jurisprudence and legal practice, as it determines the extent to which such evidence can be relied upon in criminal convictions. For

digital evidence to be accepted, a set of criteria must be met, the most important of which are authenticity—ensuring that the evidence has not been tampered with—integrity—ensuring its preservation from collection until its presentation in court—and legality—meaning that it was obtained through legal procedures .that respect individual rights

In this context, the concept of the chain of custody has emerged as a fundamental mechanism for ensuring the integrity of digital evidence, whereby all stages of handling the evidence , from its seizure to its presentation in court, are documented. Any breach of this chain of custody constitutes a potential reason for excluding the evidence due to its .unreliability

6. Digital criminal evidence in Algerian legislation

The Algerian legislator addressed the issue of proof in cybercrimes through a number of texts, most notably Law No. 09-04 relating to crimes related to information and communication technology, in addition to some amendments that affected the Code of Criminal Procedure, especially with regard to special means of investigation and electronic .search

However , practical application has revealed several problems, including the absence of detailed legal texts that precisely define the conditions for accepting digital evidence and the limits of the judge's discretion in its assessment, as well as the lack of technical training among some judges and law enforcement officers. Algerian legal scholars assert that these shortcomings could lead either to perpetrators escaping punishment or to compromising the .guarantees of a fair trial

axis : Technical, legal and procedural challenges in proving cybercrimes

1. General introduction to the problem of challenges in digital forensics

The rapid development of information and communication technology has created a new criminal reality, where crime has become more complex in terms of methods and techniques, which has directly impacted the mechanisms of criminal evidence. Despite significant advancements in digital investigation techniques, proving cybercrimes still faces a number of interconnected challenges, ranging from technical to legal to procedural. The danger of these challenges lies in their potential to render criminal laws ineffective if they are not addressed within a comprehensive legislative and institutional framework that keeps pace with the accelerating digital transformation .[14]

becomes more complicated when it comes ,to cybercrimes of a transnational nature where legal systems overlap and jurisdictions clash, making criminal proof in this area one of the most sensitive and problematic issues in contemporary criminal law .

2. Technical challenges in proving [15]cybercrimes

Technical challenges are among the most significant obstacles to prosecuting cybercrimes, as digital crimes are often committed using highly sophisticated methods that enable perpetrators to conceal their identity or erase their electronic traces with relative ease. The adoption of technologies such as Virtual Private Networks (VPNs) , anonymity software, and advanced encryption makes tracking down perpetrators a complex technical matter requiring highly specialized tools and expertise .

Furthermore , the dynamic nature of digital data presents a significant obstacle to proving wrongdoing, as evidence can be deleted or altered in seconds without leaving a clear physical trace. This challenge is exacerbated by the proliferation of cloud storage technologies , where data related to a crime is stored on servers outside the national territory and subject to foreign laws that may not allow easy access .[16]

Furthermore, some law enforcement ,agencies, particularly in developing countries have limited technical capabilities, where advanced technology and qualified personnel capable of collecting and analyzing digital evidence according to internationally recognized scientific standards are not always available. This deficiency sometimes leads to

the loss of evidence or casts doubt on its admissibility in court .

3. Legal challenges related to the admissibility of digital evidence

,In addition to technical challenges criminal evidence in cybercrimes faces profound legal challenges, primarily related to the absence or inadequacy of a legislative framework governing digital evidence. In many legal systems, traditional texts on criminal evidence remain unable to accommodate the specific technicalities of digital evidence, leaving ample room for unstable judicial interpretation .[17]

One of the most significant challenges lies in determining the legal value of digital evidence, particularly data extracted from private communication channels such as email or messaging applications. The question arises as to whether this data constitutes written evidence or merely technical circumstantial evidence requiring corroboration. This issue is further exacerbated by the lack of standardized criteria for assessing the reliability of digital evidence .[18]

also arises, as the competent authorities ,must respect constitutional guarantees foremost among them the right to privacy and the confidentiality of communications. Any violation of these guarantees leads to the exclusion of evidence, even if it reveals the truth, thus placing the judiciary in a difficult position of balancing the requirements of combating crime with the protection of individual rights and freedoms .

4. Procedural challenges in collecting [19]and analyzing digital evidence

Criminal procedures related to the collection of digital evidence represent one of the most significant weaknesses in combating ,cybercrime. Electronic searches, for example differ fundamentally from traditional searches, as they are not limited to a specific physical location, but may include interconnected information systems, remotely stored data, and multiple cloud accounts .

raises practical issues related to defining the scope of the search, ensuring that the limits of the judicial warrant are not exceeded, and how to document the seizure process in a way that guarantees the integrity of the digital evidence. Furthermore, the absence of standardized procedural protocols for collecting digital evidence could invalidate the procedures or cast doubt on their integrity .

The issue of judicial expertise is also prominent , as courts increasingly rely on technical expert reports to interpret digital evidence. However, varying levels of expertise, or the absence of clear standards for expert accreditation, can negatively impact the quality of evidence and undermine the judge's confidence in the technical findings presented .

5. Challenges associated with the transnational nature of cybercrime

Cybercrime is characterized by its transnational nature, where a criminal act can be committed in one country, its effects in another, and its data stored in a third. This geographical dispersion is one of the most serious challenges facing criminal investigations, as it raises complex issues related to jurisdiction, conflict of laws, and international cooperation .[20]

In this context, the judiciary faces significant difficulties in obtaining digital ,evidence located outside national territory particularly given the differences in legal systems and the varying levels of judicial cooperation between countries. Despite international efforts to enhance cooperation in this area, procedures often remain slow, which is at odds with the rapid deterioration of digital evidence .[21]

6. The impact of these challenges on criminal policy

The numerous challenges associated with proving cybercrimes have led to a rethinking of contemporary criminal policy, as punitive measures alone are no longer sufficient to combat this type of crime. A comprehensive approach is now essential, one that includes updating legislation, enhancing technical capabilities, developing international cooperation, and investing in the development of qualified human resources .[22]

In this context, it is noteworthy that some comparative legislations have moved towards establishing specific rules for digital forensic

evidence and explicitly recognizing the admissibility of digital evidence, provided that standards of integrity and legality are respected. This trend indicates a gradual shift ,towards a more flexible system of evidence one better equipped to accommodate digital [23].transformations

axis : International experiences and modern approaches in proving cybercrimes

1. General introduction to the importance of international experiences in developing digital forensic evidence

Given the increasing complexity of cybercrime, national legislative or procedural solutions are no longer sufficient to address ,the challenges of criminal evidence. Instead drawing on international experiences and comparative approaches has become a scientific and practical necessity. International experiences allow us to identify best practices in the collection and evaluation of digital evidence, and to anticipate emerging trends that can contribute to the development of national legal systems, particularly in countries whose legislation in this area is still under development or modernization .[24]

lies in the fact that it highlights the global shift towards the increasing recognition of digital evidence and the standardization of how to deal with it, while striving to achieve a delicate balance between the effectiveness of criminal prosecution and the protection of fundamental rights, foremost among them the right to privacy and a fair trial .[25]

2. The European experience in proving cybercrimes

The European experience is among the most advanced in the field of criminal evidence for cybercrimes, thanks to the integrated legal and institutional framework adopted by the Council of Europe and the European Union. The 2001 Budapest Convention on Cybercrime formed the cornerstone of this framework, establishing uniform rules for criminalizing cyber acts and regulating specific mechanisms for collecting and preserving digital evidence, particularly through expedited data preservation procedures and cross-border electronic forensics .[26]

European courts, particularly the European Court of Human Rights, have adopted a flexible approach to evaluating digital evidence, focusing more on the physical form of the evidence than on the extent to which legal procedures and fundamental safeguards have been respected. This is evident in judicial rulings that affirm the legitimacy of digital evidence based on the principle of proportionality between the requirements of criminal investigation and the protection of privacy, which has contributed to strengthening judicial confidence in digital evidence without compromising the rights of the defense .[27]

The European Union has also worked to strengthen judicial cooperation in the digital field through mechanisms such as the European Order for Access to Electronic Evidence, which aims to accelerate judicial authorities' access to data stored by digital service providers, while respecting rules .[28] relating to the protection of personal data

3. The American experience in digital forensics

The American experience in prosecuting cybercrimes is characterized by its practical and pragmatic nature, placing great importance on developing digital investigation techniques and emphasizing the role of technical expertise in criminal evidence. The American legal system relies heavily on digital evidence extracted from electronic ,devices and communication networks provided that the principle of legality is strictly adhered to, particularly regarding obtaining prior judicial authorization for electronic searches and surveillance .

American judicial precedent has contributed to establishing precise standards for the admissibility of digital evidence, based on verifying the integrity of the collection procedures, ensuring the chain of transmission, and demonstrating the reliability of the technical means used. Furthermore, the American judiciary has increasingly relied on expert testimony in the field of digital evidence, considering a judge's understanding

of the technical aspects a prerequisite for forming a sound judicial opinion .

The American experience is considered an advanced model in integrating technology within the criminal justice system, where specialized cybercrime units have been ,established within law enforcement agencies along with ongoing training programs for judges and members of the Public Prosecution in the field of digital evidence .

4. Comparative experiences in Arab countries

At the Arab level, recent years have witnessed a notable increase in interest in cybercrimes and the challenges of proving them, although this development remains uneven across different countries. Some Arab legislations have moved towards enacting ,laws specifically addressing cybercrimes explicitly recognizing the admissibility of digital evidence and establishing special procedures for electronic searches and seizures .[29]

However, the practical application of digital technology in many Arab countries still faces challenges related to weak technological infrastructure, a shortage of specialized expertise, and limited judicial practice in this area. It is also observed that some Arab courts ,are cautious in accepting digital evidence sometimes leading to its exclusion or a reduction in its evidentiary value. This reflects the urgent need to develop judicial training and enhance confidence in modern technologies .

5. Modern approaches to proving cybercrimes

Rapid technological advancements have given rise to modern approaches in digital forensics, employing advanced tools such as artificial intelligence and big data analytics in criminal investigations. Some judicial systems now rely on specialized algorithms to analyze massive amounts of digital data and extract behavioral patterns that may contribute to solving complex cybercrimes .[30]

proactive evidence approach , which relies on collecting and preserving digital data before it is lost, has also emerged through legal mechanisms that allow competent authorities to issue orders for the immediate preservation of data with digital service providers. This approach aims to overcome the problem of the rapid deterioration of digital evidence and ensure its availability when needed in court .[31]

In the same context, the rules of evidence have witnessed remarkable development through the increasing recognition of the digital storage chain, and the adoption of unified technical standards to ensure the integrity of digital evidence, which enhances its credibility before the judiciary and reduces challenges related to data manipulation or distortion .[32]

6. A critical assessment of the potential for benefiting from international experiences in Algeria

A study of international experiences and modern approaches clearly demonstrates that developing criminal evidence in cybercrimes cannot be done in isolation from the national context, whether in terms of the legal framework or the available technical and human resources. For Algeria, benefiting from these experiences requires adapting them to the specificities of its national legislation and institutions, rather than simply adopting them verbatim .

Strengthening international cooperation and actively participating in regional and international mechanisms for combating cybercrime are essential steps to overcome the challenges associated with the transnational , nature of digital evidence. Furthermore investing in the training of judges and law enforcement officers in digital investigations is a fundamental prerequisite for the success .of any legislative reform in this area

Fifth axis: The reality of Algeria and policy recommendations in the field of proving cybercrimes

1. A general introduction to the reality of criminal evidence in cybercrimes in Algeria

Like other countries, Algeria has witnessed a significant rise in cybercrime in recent years, driven by the widespread use of information and communication technologies and the rapid shift towards digitalization

across various sectors. This reality has presented new challenges to the criminal justice system, particularly regarding its capacity to prove these types of crimes, which are characterized by their technical complexity and the intangible nature of the evidence .

The reality of criminal evidence in cybercrimes in Algeria is a direct reflection of the extent to which the legal and institutional ,system has adapted to digital transformations as there is a clear disparity between legal texts on the one hand, and practical application on the other, which calls for an objective analysis that identifies strengths and weaknesses, in preparation for proposing effective policy recommendations .

2. The legal framework governing the proof of cybercrimes in Algeria

constituted a significant step in the .modernization of Algerian criminal policy This law established a set of investigative and prosecution mechanisms, including interception of communications, electronic .searches, and the preservation of digital data This framework was further strengthened by amendments to the Code of Criminal Procedure, which allowed for the use of specialized investigative methods suited to the nature of emerging crimes .

However, an analytical reading of these texts reveals that the Algerian legislator focused primarily on procedural and deterrent aspects, without establishing detailed regulations concerning the admissibility of digital evidence and the criteria for its acceptance and evaluation in court. It is noteworthy that Algerian judges still largely ,rely on the general rules of criminal evidence which may raise practical problems when dealing with complex digital evidence requiring specialized technical expertise .

3. The practical reality of digital criminal evidence before the Algerian judiciary

reveals that proving cybercrimes still faces several practical difficulties, primarily related to the collection and analysis of digital evidence. Despite the efforts of security services, technical and human resources remain insufficient in some cases to keep pace with the rapid evolution of cybercrime methods .

The Algerian judge also relies heavily on ;expert technical reports to form his conviction however, the varying levels of expertise among experts and the absence of unified national standards for accreditation and evaluation can sometimes lead to conflicting findings or cast doubt on the credibility of the presented evidence. Furthermore, the limited body of published judicial precedent in the field of cybercrime reduces the potential for establishing stable legal principles related to digital evidence .

4. The problem of balancing the requirements of proof with the protection of rights and freedoms

,Protecting individual rights and freedoms especially the right to privacy and confidentiality of communications, is one of the most significant challenges facing criminal investigations in cybercrimes in Algeria. The use of special investigative methods, such as ,electronic surveillance and data interception raises legitimate concerns about the potential ,infringement on individuals' privacy particularly in the absence of rigorous judicial oversight or clear standards defining the scope of these procedures .

imposes on Algerian criminal policy the need to achieve a delicate balance between the effectiveness of combating cybercrimes and ensuring respect for constitutional rights, a balance that can only be achieved through clear texts, stable judicial interpretation, and effective oversight mechanisms for the work of the judicial police .

5. Requirements for developing digital forensic evidence in Algeria

Developing the system of criminal evidence in cybercrimes in Algeria requires a comprehensive approach that goes beyond partial or ad hoc solutions. The challenges at hand cannot be addressed simply by increasing penalties or expanding investigative powers; rather, they necessitate structural reform encompassing the legal framework, institutional structure, and human resource development .

is highlighted , whether for judges, public prosecutors, or judicial police officers, as a deep understanding of the technical aspects is essential for the proper evaluation of digital evidence. Furthermore, integrating modern technologies into judicial work, such as digital evidence management systems, enhances the efficiency of investigations and ensures the integrity of evidence .

6. Policy recommendations to enhance the effectiveness of criminal evidence in cybercrimes

In light of the preceding analysis, there is a clear need to adopt a set of policy recommendations that would enhance the effectiveness of criminal evidence in cybercrimes in Algeria. Foremost among these recommendations is the necessity of completing the legislative framework by enacting explicit provisions that recognize the admissibility of digital evidence and define the conditions for its collection, preservation, and evaluation, in accordance with international standards and respecting constitutional guarantees .

also recommended to establish specialized digital investigation units within judicial and security agencies, equipped with modern .technology and qualified personnel Strengthening international cooperation, both bilaterally and multilaterally, is essential to addressing the transnational nature of cybercrime, particularly in the exchange of digital evidence .

Among the essential recommendations is also the development of a national guide to procedures relating to digital evidence, which defines the technical and legal standards to be followed, in order to ensure the standardization of practices and enhance the .judiciary's confidence in this type of evidence

General Conclusion

Modern cybercrimes have become one of the most serious challenges facing criminal justice systems in the digital age, given their ,technical complexity, transnational nature and rapid evolution that often outstrips the .ability of traditional legislation to keep pace This reality has created profound problems in criminal evidence, as evidence is no longer confined to its familiar physical form, but has become largely intangible, ephemeral, and tamper-proof digital evidence, requiring ,specialized technical expertise to extract analyze, and present it in court .

The study revealed that the effectiveness of combating cybercrime depends not only on ,criminalizing newly emerging acts, but also and more fundamentally, on the procedural system's ability to accommodate modern methods of evidence. This necessitates a balance between the demands of effective criminal prosecution and the safeguards for fundamental rights and freedoms, most importantly the right to privacy and the ,confidentiality of personal data. Furthermore a comparison of international experiences showed that countries that have been relatively successful in curbing these crimes are those ,that have adopted a comprehensive approach ,combining legislative modernization ,specialized training, international cooperation and the development of the technological infrastructure of judicial and security institutions .

In the Algerian context, despite the legislative efforts made, particularly through the law relating to the prevention and combating of crimes related to information and communication technologies, the practical reality reveals the continuation of a number of difficulties related to the admissibility of digital evidence, the lack of technical expertise, and the weakness of international coordination, which calls for deep reforms that go beyond partial or circumstantial treatment .

Therefore, enhancing the effectiveness of criminal evidence in the field of modern cybercrimes remains contingent on adopting an integrated strategic vision that incorporates the technical dimension into the core of criminal justice, without compromising the foundations of a fair trial and the principles of the rule of law .

Recommendations

First: Legislative recommendations

It is recommended that the penal and procedural texts be reviewed and updated in ,line with the changing nature of cybercrimes with an explicit stipulation of the admissibility of digital evidence and the rules for its acceptance and judicial evaluation, and the standardization of relevant technical terms to avoid differing interpretations .

Second: Judicial and procedural recommendations

should be strengthened by establishing specialized departments or judicial divisions for cybercrimes, with the training of judges and public prosecutors in the field of digital evidence and electronic investigation methods, in order to ensure the proper assessment of this type of evidence .

Third: Technical and institutional recommendations

It is recommended to strengthen digital evidence laboratories and equip them with .sformations modern technologies, while adopting unified scientific standards in collecting, analyzing and preserving digital evidence, ensuring its integrity and chain of legal possession, and preventing challenges to its legitimacy .

Fourth: Recommendations related to the protection of rights and freedoms

It is necessary to establish a delicate balance between the requirements of investigating cybercrimes and ensuring the protection of privacy, by subjecting electronic surveillance and digital inspection procedures ,to prior and justified judicial authorization and activating subsequent judicial oversight .

Fifth: Recommendations at the level of international cooperation

Strengthening international judicial and security cooperation mechanisms, and actively engaging in international agreements related to cybercrimes, allowing for the exchange of digital evidence and the extradition of criminals, especially in cross-border crimes .

Sixth: Research and academic recommendations

Encouraging specialized scientific research in the field of digital evidence, and linking universities with judicial and security institutions, in order to produce legal and technical knowledge capable of keeping pace with rapid digital tran

---

[1] Hussam Ahmed Kilani, Digital Evidence and Obstacles to Proving Cybercrime, Journal of Jurisprudential and Legal Research , 2024 .

[2] Council of Europe, Convention on Cybercrime , Budapest, 2001

[3] ,Abdelhamid Makhokh and Boualem Belfar , Proof of Cybercrimes in Algerian Legislation, Master's Thesis Mohamed El Bachir El Ibrahimi University, 2024

[4] Wahiba Laouarem, Digital Evidence in the Field of Criminal Proof According to Algerian Legislation, National Criminal Journal, 2023 .

[5] Law No. 09-04 relating to crimes related to information and communication technologies, Algeria .

[6] Rihab Yousfi and Wahiba Louarem , "Digital Evidence and Proving Cybercrime ," International Tax Journal, 2025.

[7] Hussam Ahmed Kilani, Digital Evidence and Obstacles to Proving Cybercrime, Journal of Jurisprudential and Legal Research , 2024 .

[8] Abdul Hamid Makhokh , Criminal Evidence in Cybercrimes, Dar Al-Jami'a Al-Jadeeda, 2023 .

[9] Council of Europe, Electronic Evidence Guide, 2022.

[10] Wahiba Laawarim, The Admissibility of Digital Evidence in Criminal Proof, National Criminal Journal, 2023 .

[11] Rihab Yousfi & Wahiba Louarem , "Digital Evidence and Criminal Proof," International Journal of Law and Technology , 2025.

[12] Algerian Code of Criminal Procedure .

[13] Law No. 09-04 relating to crimes related to information and communication technology .

[14] Susan W. Brenner, Cybercrime and the Law: Challenges, Issues, and Outcomes (Boston: Northeastern University Press , 2019), 85–88.

[15]United Nations Office on Drugs and Crime (UNODC), Comprehensive Study on Cybercrime (Vienna: UNODC, 2021), 149–153.

[16] Eoghan Casey, Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet (London: Academic Press , 2020), 61–64.

[17]Jean-François Blanchette, "The Materiality of Digital Evidence," Journal of Digital Forensics 15, no. 3 (2021): 74–79.

[18] ,Abdel Hamid Makhokh , Criminal Evidence in Cybercrimes (Alexandria: Dar Al-Jami'a Al-Jadeeda, 2023) 101–97 .

[19] Hussam Ahmed Kilani , "The Problem of Criminal Evidence in Cybercrimes", Journal of Jurisprudential and Legal Research, Issue 13 (2024): 133–136 .

[20] Wahiba Laouarem, "The Legality of Digital Evidence Between Security Requirements and Privacy Protection", Algerian Journal of Legal Sciences, Issue 2 (2023): 112 .

[21] Abdelkader Bouarfa, "Procedural Challenges in Combating Transnational Cybercrimes", Algerian Journal of Legal and Political Sciences, No. 1 (2024): 66–69 .

[22] Ahmed Fathi Sorour, The Mediator in Criminal Procedure Law (Cairo: Dar Al Shorouk, 2018), 731–735 .

[23] Nadezhda Purtova , "Cross-Border Access to Digital Evidence and Jurisdictional Conflicts ," European Data Protection Law Review 7, no. 4 (2021): 505–510.

[24] Council of Europe, Convention on Cybercrime (Budapest Convention) (Budapest, 2001), arts. 16–21.

[25]Council of Europe, Electronic Evidence Guide: A Basic Guide for Judges and Prosecutors (Strasbourg: Council of Europe Publishing , 2022), 19–27.

[26] European Commission, European Production and Preservation Orders for Electronic Evidence in Criminal Matters (Brussels, 2018), 6–11.

[27] Nadezhda Purtova , "Cross-Border Access to Electronic Evidence and Jurisdictional Conflicts ," European Data Protection Law Review 7, no. 4 (2021): 506–514.

[28] European Court of Human Rights , Barbulescu v. Romania, no. 61496/08, Judgment of 5 September 2017, paras. 115–123.

[29]United States Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations

[30]Ali Al- Khouri , "Digital Forensics and Cybercrime Investigation: Emerging Trends," Journal of Information Security 15, no. 1 (2024): 21–28.

[31]OECD, Cybersecurity , Digital Evidence and Criminal Justice (Paris: OECD Publishing , 2022), 37–44.

[32]Jean-François Blanchette, "The Materiality of Digital Evidence," Journal of Digital Forensics 15, no. 3 (2021): 78–85.