

Evidentiary Mechanisms and Forensic Frameworks in the Investigation of Cybercrimes

Bousmaha Amina^{1*}, Saïda University, Algeria Bousmaha.amina@univ-saida.dz

Bouarfa Abdelkader², Saïda University, Algeria Bouarfa.abdelkader@univ-saida.dz

Send Article Date: 2026-01-10

Date of acceptance of the article 2026-03-27

Abstract: With the rapid advancement of internet and computer technologies across the globe, a new category of crime has emerged—cybercrime—which now poses a threat no less serious than traditional criminal activity. These offenses are notoriously difficult to detect and prove due to their occurrence in a dematerialized digital realm. Recognizing this danger, Algerian legislation, like many other legal systems, enacted Law No. 09-04 on offenses against automated data processing, and amended the Penal Code accordingly by introducing Articles 394 bis to 394 bis 7. Despite these efforts, investigative authorities still face significant challenges in gathering tangible and admissible evidence in cybercrime cases.

key words: : Computer, Cybercrime, Investigation, Forensic Evidence.

Introduction:

The exponential advancement in the domain of information technologies has engendered a paradigmatic digital revolution, heralding the emergence of a novel and formidable category of criminal phenomena, now commonly referred to as *cybercrime* or *computer-mediated criminality*. What renders this form of delinquency particularly alarming is not merely the technical sophistication it entails, but rather the unparalleled ease and rapidity with which such offenses may be perpetrated—often within mere moments—coupled with the perpetrator's capacity to obliterate digital traces with exceptional stealth and expediency.

Moreover, cyber-offenders—especially those operating within the intricate architectures of transnational organized crime—frequently resort to encrypting incriminating data or concealing evidence within highly fortified digital systems. These systems are often engineered to resist conventional investigative techniques, thereby posing profound evidentiary and procedural challenges to criminal justice authorities in their quest to gather, preserve, and authenticate proof of culpability.

In consequence, the association of cybercrime with computer systems and digital infrastructures not only differentiates it substantially from conventional criminal modalities but also necessitates the conceptual and operational reconfiguration of the profile of the cybercriminal—who typically embodies a distinct set of cognitive, technical, and behavioral traits, divergent from the stereotypical offender engaged in analog criminality.

Equally significant is the divergence in evidentiary mechanisms. The nature, scope, and admissibility of investigative tools in cybercrime cases markedly differ from those traditionally employed in the context of physical or tangible offenses. This necessitates a re-evaluation of legal doctrines pertaining to digital forensics, procedural safeguards, and evidentiary thresholds.

This chapter therefore endeavors to explore and analytically deconstruct the evidentiary frameworks applicable to cybercrime investigations, with particular emphasis on the dichotomy between traditional investigative methodologies and the emergent, technologically adaptive

instruments tailored for digital offenses. It seeks to assess the extent to which Algerian legislative instruments—most notably Law No. 09-04 concerning offenses against automated data processing systems—have risen to the occasion in confronting this complex legal and technological landscape.

Section One: Traditional Evidentiary Tools in Criminal Investigations Pertaining to Cybercrimes

Despite the technological novelty inherent to cybercriminal conduct, there exists a substantive procedural parallelism between investigative methodologies applicable to internet-facilitated offenses and those traditionally employed in response to conventional criminal acts. In both contexts, investigative authorities are compelled to rely upon foundational evidentiary procedures, including on-site inspection (*locus delicti* examination), forensic searches, witness testimonies, expert evaluations, and systematic evidence gathering. These procedural pillars remain the bedrock of criminal fact-finding, regardless of the medium through which the offense is perpetrated.

Indeed, such conventional investigative techniques constitute the procedural nucleus of fact-establishing operations deployed by law enforcement and prosecutorial bodies. These mechanisms are not merely formalistic rituals; rather, they are indispensable instruments for uncovering material facts, identifying perpetrators, securing the chain of custody, and facilitating the eventual adjudication of justice before the competent judicial authorities. The probative weight of each of these tools—be it inspection, search, testimony, or circumstantial inference—is contingent upon strict adherence to codified legal standards and procedural safeguards.

However, the Algerian legislator, acutely cognizant of the nuanced nature of cyber-related offenses, has extended the ambit of traditional evidentiary procedures by incorporating additional safeguards and mechanisms tailored to the digital context. Through the enactment of Law No. 09-04, addressing offenses against information and communication technologies, and its harmonization with the Code of Criminal Procedure, the legislator has delineated specific provisions regulating search and seizure operations within digital environments. These norms are designed to bridge the conceptual and procedural gap between conventional physical evidence and its intangible digital counterparts.

Subsection One: Scene Examination (*La Constatation*) as a Form of Evidentiary Inquiry

At its core, scene examination—referred to in legal parlance as *constatation*—constitutes a procedural device aimed at achieving immediate sensory engagement with the physical or circumstantial elements of the crime scene. It enables the investigative authority to directly perceive the spatial and material configuration of the crime locus, thereby extracting probative cues capable of shedding light on the event in question.

This procedural step, which oscillates between evidentiary collection and preliminary inquiry, serves as a conduit for reconstructing the narrative of the offense through the physical residues and contextual elements present at the scene. The objective is to meticulously catalog fixed and movable elements—whether physical objects, biological traces, or spatial displacements—that may signify the occurrence of criminal conduct, in order to derive legal inferences from their presence or configuration¹.

1. Definition of Scene Examination

Judicial doctrine defines *scene examination* as the process whereby an investigating magistrate or designated official undertakes a direct and unmediated appraisal of the physical milieu associated with the criminal act. This may entail documenting material consequences of the offense, inspecting relevant objects or individuals, and establishing the contextual backdrop

within which the crime unfolded—including, but not limited to, the instrumentalities employed and the spatial or temporal coordinates of the incident².

More specifically, it encompasses both the act of relocating to the locus of the offense and, conversely, transporting evidentiary objects to the investigator's premises. It applies to diverse scenarios such as the inspection of counterfeit currency, examination of weapons or forged documents, forensic analysis of bodily injuries sustained by the victim, or medical scrutiny of the accused in cases involving torture or bodily harm.

The significance of this procedural mechanism is accentuated in the immediate aftermath of a conventional criminal event, wherein the integrity of the crime scene is paramount. The investigator bears the procedural and ethical obligation to secure the evidentiary ecosystem against contamination or loss, thereby preserving the authenticity of material clues³.

In sum, scene examination enables judicial authorities to apprehend the crime and its perpetrator in a direct, tangible manner. It also allows for the verification of consequential elements left in the wake of the offense and the reconstruction of its operational dynamics.

2. Scene Examination in Cybercrime Investigations

Although scene examination plays a pivotal role in elucidating the factual matrix of traditional offenses, its applicability within the cybercrime domain is significantly attenuated. This procedural limitation is attributable to a number of factors:

- Firstly, cybercrimes—particularly those perpetrated through networked infrastructures—seldom leave behind discernible material traces that can be physically apprehended or preserved.
- Secondly, the temporal latency between the commission of the digital offense and the initiation of investigative procedures frequently allows for contamination, alteration, or obliteration of digital residues, especially in settings subject to high traffic or public access.

In recognition of these vulnerabilities, the Algerian legislature, through Article 43 of the Code of Criminal Procedure, has codified specific protections aimed at preserving the integrity of the crime scene, even in the context of digital or hybrid offenses⁴. The provision stipulates that:

"Any unauthorized person who alters the condition of the premises or removes any object from the scene of a felony prior to the initiation of official investigative measures shall be subject to a monetary fine ranging from 200 to 1,000 Algerian dinars".

This legal norm reflects a commitment to evidentiary sanctity, emphasizing that the preservation of the crime scene remains a non-negotiable precondition for legitimate forensic intervention—regardless of whether the underlying offense is analog or digitally mediated.

Subsection Two: Digital Search as an Evidentiary Instrument in Cybercrime Investigations

Search operations constitute a foundational pillar within the procedural arsenal of criminal investigation, particularly in the context of cybercrime, wherein digital environments substitute physical reality, and data replaces traditional tangible evidence. The Algerian legislator, in recognition of the unique exigencies that characterize electronic evidence, has explicitly addressed the legal framework surrounding searches in the digital sphere through Law No. 09-04, particularly in Articles 5(4) and 6(3), which confer upon competent authorities the right to perform forensic searches—remotely if necessary—within computerized systems and data repositories⁵.

1. Definition and Legal Nature of Search Procedures

Doctrinally, a search may be defined as a state-authorized intrusion into the suspect's private domain—commonly conceptualized as the "repository of secrets"—with the intent to discover concealed evidence or individuals evading justice. As such, it is not a preemptive measure but a reactive procedural tool, activated upon the occurrence or reasonable suspicion of a criminal offense. It entails a systematic and purposeful exploration of environments, persons, or data likely to yield incriminating material⁶.

Searches inherently engage with the private and often constitutionally protected spheres of human activity. Unlike objects accessible to the public eye, search targets are typically hidden within residences, personal devices, or encrypted systems. Consequently, a legitimate search must be warranted, proportional, and guided by legal due process to ensure its evidentiary admissibility and constitutional compliance.

From a functional standpoint, searches are aimed at identifying and securing evidence relevant to the crime under investigation. This evidence may include physical objects, biometric traces, or, in the digital realm, intangible datasets encoded within electronic infrastructures. The latter, in particular, raise profound jurisprudential questions, notably regarding the materiality and legal recognition of non-physical evidence⁷.

2. Digital Searches and the Problematization of Immaterial Evidence

The legal conception of search operations does not undergo fundamental alteration in the context of cybercrime. However, its application is rendered complex by the dematerialized nature of the objects of the search. Entering a digital system—whether a local server, cloud environment, or decentralized blockchain network—requires a technical and legal framework that allows for the extraction of data without compromising its authenticity.

Two dominant interpretative currents have emerged in legal doctrine:

- The expansive-materialist interpretation argues that digital programs and datasets, while immaterial in appearance, possess material properties by virtue of their physical storage in computer memory. This view posits that digital evidence occupies measurable space (e.g., bytes)⁸ and should thus be subsumed under the notion of "things" capable of being searched and seized⁹.
- The legal-reformist interpretation highlights the conceptual limitations of traditional procedural statutes in addressing cyber investigations. It advocates for legislative innovations that explicitly incorporate data processing materials into the scope of searchable objects¹⁰. According to this school, the search of a digital environment must be recognized as an autonomous procedure adapted to the particularities of cyberspace¹¹.

The Algerian legislator has substantively aligned with both perspectives by criminalizing unauthorized interference with automated data processing systems under Law No. 04-15 and by legitimizing digital searches under Law No. 09-04¹². Specifically, Article 5 authorizes judicial and police authorities to remotely access and search digital systems and databases within the framework of existing criminal procedural laws¹³.

To be lawful, a digital search must be predicated upon a verified cyber offense of sufficient gravity—felonies and misdemeanors are included, whereas minor infractions are excluded. Moreover, the legality principle in penal law prohibits investigative measures unless the conduct under scrutiny is explicitly criminalized.

The search of physical electronic components—such as hardware, peripherals, and communications devices—is uncontroversial under Articles 44 to 64 of the Code of Criminal Procedure. These articles permit searches targeting "objects," a term interpreted to include

tangible electronic devices. The legality of such searches, however, depends on the nature of the location—whether public or private—and must conform to established procedural safeguards. Law No. 06-22¹⁴ introduces exceptions to procedural guarantees, especially in cases involving crimes against data processing systems. Here, the public interest and collective security justify a recalibration of individual privacy rights, particularly in emergency contexts where rapid data destruction may preclude traditional warrant procedures¹⁵.

Nonetheless, significant procedural obstacles persist:

- The decentralized architecture of information systems, with data stored across multiple jurisdictions.
- The limited technical expertise of certain investigators.
- The difficulty in defining and delimiting the precise object of the search within vast digital repositories.

In conclusion, digital searches must extend to both physical and logical components of computer systems, including internal storage, software environments, and network infrastructures. Legal frameworks must evolve in tandem with technological realities to safeguard both investigatory efficacy and fundamental rights.

Subsection Three: Seizure as a Forensic Mechanism in Cybercrime Investigations

The act of seizure represents the procedural culmination of a search operation and serves as a direct legal mechanism for preserving evidence that may be instrumental in establishing criminal liability. In the context of cybercrime, seizure extends beyond the physical confiscation of devices to encompass the capture and duplication of intangible digital assets, such as data, programs, and metadata.

1. The Legal and Evidentiary Function of Seizure

Seizure is defined as the act of taking possession of an item related to a criminal offense, with the intent of preserving it for evidentiary analysis and eventual judicial use. As such, it shares the procedural prerequisites of a search and is rendered invalid if the underlying search is unlawful. Its purpose is to secure items—physical or digital—that bear probative value in reconstructing the criminal event and identifying the perpetrator.

In the cyber domain, physical components subject to seizure include computers, storage devices, routers, modems, and any ancillary hardware¹⁶. These items may be removed or inspected in situ, depending on logistical constraints and legal authorizations. Notably, the seizure of entire systems is not always necessary; often, the duplication of relevant data to secure digital storage media suffices¹⁷.

The Algerian legislative framework addresses digital seizure under Article 6 of Law No. 09-04. This provision stipulates that when authorities conducting a search identify stored data that may illuminate the facts of the case or the identity of the offender, they may extract and secure said data on appropriate digital media, in accordance with the procedural requirements of the Code of Criminal Procedure¹⁹.

2. Procedural Implementation of Digital Seizure

Article 6 of Law No. 09-04 delineates two principal functions of digital seizure²⁰:

- Evidence acquisition and preliminary analysis: The primary objective is to obtain and preserve data likely to be of evidentiary value. This necessitates identifying data sources, extracting content, and ensuring its forensic integrity through cryptographic hashing or other verification methods.
- Preventive confiscation and data preservation: Authorities may isolate original datasets, duplicate them for analysis, and restrict access to the originals. Importantly, seizure does

not entail deletion or destruction; on the contrary, it aims to preserve data in its native form for future judicial scrutiny.

The integrity of the data environment must be maintained throughout the seizure process. Authorities are permitted to use technical means to reformat or reconstruct data, provided such interventions do not compromise evidentiary integrity. Where technical limitations preclude immediate seizure, authorities may implement access restrictions or encryption to prevent unauthorized manipulation.

In sum, digital seizure is not merely a technical operation but a complex legal act requiring stringent procedural compliance, technological competence, and a robust normative foundation. The Algerian legal framework demonstrates a progressive orientation in this regard, but continuous reform is necessary to keep pace with the evolving landscape of cyber delinquency and digital forensics²¹.

Section Two: Emerging Evidentiary Mechanisms in the Criminal Investigation of Cybercrimes

In the contemporary digital epoch—marked by the ubiquity of information and communication technologies across domains such as e-commerce, e-banking, and e-governance—cybercrime has emerged not merely as a peripheral threat but as a systemic hazard capable of undermining the structural integrity of national security, public order, and economic stability. As the frequency and complexity of cyber-enabled offenses proliferate, including acts of cyber espionage, cyberterrorism, political incitement via digital platforms, and sophisticated forms of electronic forgery and fraud, states are compelled to recalibrate their criminal justice strategies. This recalibration necessitates the deployment of novel evidentiary modalities capable of navigating the unique epistemological terrain of cyberspace.

The distinctiveness of cybercriminal conduct—particularly its transboundary character, its reliance on anonymizing technologies, and its propensity for evidence volatility—necessitates the formulation of investigative tools that are both technologically responsive and legally defensible²². Consequently, the Algerian legal system has begun to integrate advanced techniques such as the surveillance of electronic communications, the interception of data flows, and the expedited preservation of stored digital content, thereby constituting a second generation of forensic evidentiary mechanisms.

Subsection One: Electronic Communications Surveillance as an Evidentiary Technique

The exponential expansion of digital infrastructures in Algeria and globally has given rise to emergent categories of criminal conduct that threaten the foundational pillars of social cohesion and sovereign authority. In response, the Algerian legislator introduced a legal innovation through Law No. 06-22, dated 20 December 2006, amending the Penal Code to incorporate technologically enhanced methods of criminal investigation, most notably the surveillance of electronic communications.

1. Conceptual Definition of Electronic Surveillance

Electronic surveillance refers to the procedural act of systematically collecting, recording, accessing, and analyzing the content of electronic communications. Codified in Law No. 04-09 of 5 August 2009, concerning the prevention and suppression of ICT-related offenses, such surveillance is governed by a specific set of procedural safeguards despite its inherent encroachment upon individual liberties and the sanctity of private life.

The essence of surveillance lies in the aggregation of digital correspondence—including emails, messages, and telephonic exchanges—and the subsequent forensic review of their contents. These communications frequently encapsulate sensitive and private information, rendering

surveillance not only a potent investigative mechanism but also a potential infringement upon constitutionally protected rights.

While the legislator refrains from exhaustively enumerating the permissible technological methods, Law No. 09-04 implicitly requires the establishment of specialized technical arrangements to regulate surveillance operations. Notably, Article 4 of said law specifies, in a numerus clausus manner, the scenarios under which electronic surveillance may be lawfully executed:

- Prevention of acts categorized as terrorism, sabotage, or those endangering state security.
- Situations involving credible threats to information systems that jeopardize public order, national defense, institutional integrity, or the national economy.
- Judicial investigations where alternative methods fail to yield actionable intelligence, particularly in the context of international legal cooperation.

2. Judicial Safeguards Governing Surveillance Operations

Given that electronic surveillance inherently involves the extraction and interpretation of data with personal and potentially exculpatory significance, its legal legitimacy is contingent upon a robust framework of procedural guarantees. The act of monitoring an individual's digital behavior—whether telephonic or online—carries the risk of violating personal data protections and undermining the right to privacy²³.

In recognition of these risks, Law No. 09-04 incorporates specific judicial safeguards:

- **Judicial Oversight:** Article 4(2) stipulates that no surveillance operation may commence absent a written warrant issued by the *Procureur de la République* (Public Prosecutor). In cases involving terrorism, sabotage, or cyberattacks against automated data processing systems, the authority to authorize surveillance is vested in the *Procureur Général* of the Court of Algiers²⁴. The authorization is valid for six months and may be renewed upon submission of a technical report detailing the nature and intended purpose of the surveillance mechanisms employed²⁵.
- **Restrictive Scope of Data Utilization:** The surveillance infrastructure must be narrowly tailored to collect and record data strictly pertinent to the scenarios enumerated in Article 4—chiefly, acts of high gravity such as terrorism and systemic cyber threats. Technologies employed in this context include the interception of electronic communications, image capture, and, where appropriate, the partial or complete search and seizure of information systems, as authorized under Articles 5 and 7 of Law No. 09-04²⁶.

These safeguards are designed to strike a delicate balance between the imperatives of state security and the inviolability of private life. They serve to legitimate the evidentiary use of intercepted communications in judicial proceedings while minimizing the risk of arbitrariness and abuse of power.

Subsection Two: The Interception of Electronic Communications as Legal Evidence in Cybercrime Investigations

The contemporary landscape of criminal investigation has witnessed a paradigmatic shift whereby traditional investigative tools—once effective in uncovering the physical traces of criminal acts—have become largely obsolete in the face of technologically sophisticated offenses. Perpetrators of cybercrime increasingly exploit advanced scientific and technological means to commit acts that leave little or no tangible residue, rendering conventional modes of inquiry ineffective. Consequently, it has become imperative for legislatures and law enforcement agencies to adopt cutting-edge methodologies such as the interception of electronic

communications, audio surveillance, and digital image capture. These techniques, while encroaching upon constitutionally enshrined rights to privacy, have been cautiously legitimized under Algerian law, subject to a strict matrix of judicial safeguards designed to protect fundamental human rights²⁷.

1. Definition and Conceptualization of Interception

Electronic interception—broadly construed—refers to the covert or overt acquisition of data transmissions, including the content of voice calls, electronic mail, and other forms of telecommunication, as they occur or are stored within a digital infrastructure. This encompasses not only real-time interception but also retrospective access to static or dormant data such as unopened voicemail and archived email content retained by service providers.

This form of surveillance typically targets “traffic data,” that is, metadata pertaining to the transmission path, duration, origin, and destination of electronic communications. These data are essential for reconstructing the chronology and structure of digital interactions and thus constitute a critical evidentiary reservoir in the prosecutorial pursuit of cyber offenders.

National legal frameworks, including Algerian law, grant state authorities the discretionary power to intercept such communications without incurring criminal liability, provided that such actions are undertaken for the legitimate purposes of crime detection or the prevention of threats to national security—be they domestic or extraterritorial in nature.

In line with this prerogative, the Algerian Constitution affirms in Article 64 the inviolability of private life, explicitly stating that “The privacy of citizens and their honor shall be protected by law. The confidentiality of correspondence and private communications, in all their forms, is guaranteed.” This constitutional protection is further reinforced by Algeria’s adherence to international legal instruments, such as the Universal Declaration of Human Rights (1948), the International Covenant on Civil and Political Rights (1966), and the European Convention on Human Rights (1950), all of which enshrine the right to privacy and the prohibition of arbitrary interference.

2. Application of Interception in Cybercrime Contexts

The practice of intercepting telephonic conversations or digital transmissions for evidentiary purposes involves two principal techniques: (i) the interception of communications (wiretapping), and (ii) the recording of conversations using specialized technical equipment. Secret surveillance, particularly in cyber investigations, often entails clandestine access to a suspect's personal or associated telecommunications devices, allowing authorities to capture incriminating content without the suspect's knowledge²⁸.

Voice recordings may occur overtly—such as during formal interrogations—or covertly, with the use of concealed devices. The forensic value of such recordings lies in their potential to corroborate or refute oral testimony, especially in cases where defendants recant confessions previously rendered. These recordings may be collected by official investigative bodies or, under certain circumstances, by private individuals to substantiate claims in adversarial proceedings²⁹.

Technological advances have exponentially enhanced the capacity for visual surveillance as well. Long-distance imaging systems, infrared photography capable of capturing high-resolution images in darkness, and two-way mirror optics (also known as one-way mirrors) allow for discreet monitoring of subjects within private or enclosed spaces. The miniaturization of digital cameras enables covert placement in architectural fixtures or even on the human body, facilitating periodic or continuous image capture with minimal risk of detection³⁰.

The Algerian Code of Criminal Procedure, under Article 65 bis 5, delineates the offenses for which image capture may be authorized. These include narcotics trafficking, transnational

organized crime, cybercrime affecting automated data processing systems, money laundering, terrorism, currency violations, and corruption-related offenses. In such cases, the competent *Procureur de la République* may issue a warrant permitting image capture of one or more individuals located in private premises, underscoring the necessity of balancing investigative efficacy with the protection of civil liberties³¹.

Subsection Three: Expedited Preservation of Stored Data as a Forensic Mechanism

In the digital evidence lifecycle, the fragility and volatility of electronic data present a unique challenge to the integrity of criminal investigations. Recognizing the ephemeral nature of such information—often susceptible to deletion, modification, or obfuscation—contemporary legal systems have devised a critical procedural safeguard: the expedited preservation of stored data.

Codified in Chapter IV of Algerian Law No. 09-04 under the rubric “Obligations of Service Providers,” this measure constitutes a proactive and non-invasive means of freezing data in situ pending the initiation of more intrusive investigative steps, such as search or production orders³².

1. Conceptual Framework of Expedited Preservation

Expedited preservation entails a formal directive issued by a competent judicial or investigative authority, mandating that internet service providers or other custodians of electronic information retain specific categories of data under their control or in their possession. This preservation must occur in anticipation of further legal actions and serves primarily to prevent the loss, alteration, or destruction of potentially incriminating evidence³³.

The data subject to preservation typically includes static information—such as server logs, access timestamps, user identifiers, and digital artifacts stored within an information system. The scope of preservation, however, does not extend to real-time monitoring or data interception, thereby distinguishing it from more invasive surveillance methodologies.

2. Legal Basis and Practical Application

The international normative foundation for this mechanism is enshrined in Article 12 of the Budapest Convention on Cybercrime, which obligates signatory states to empower their authorities to issue legally binding orders compelling service providers to preserve specified data—particularly where there exists a substantial risk of evidence being compromised³⁴.

In the Algerian context, this obligation is mirrored in Law No. 09-04, which requires providers of digital services to comply with preservation orders upon request by the competent authority. Importantly, this procedure is not of general applicability; it is tailored to data that is reasonably believed to be vulnerable to loss or alteration and is thus limited in scope to avoid unnecessary encroachments on privacy.

From a forensic perspective, expedited preservation plays a dual role: it ensures evidentiary continuity by maintaining the integrity of digital evidence and it serves as a procedural bridge that permits a seamless transition to more intrusive investigative techniques. It also alleviates the risk of evidence spoliation in cases involving distributed networks, cloud storage, or remote servers—scenarios where jurisdictional and technical complexities often obstruct timely data acquisition³⁵.

Given the challenges posed by cybercrime—such as the cross-border nature of evidence, the proliferation of anonymization tools, and the rapid obsolescence of digital trails—the preservation mechanism is not merely ancillary but central to any robust digital criminal justice architecture³⁶.

Conclusion

Over the past three decades, the personal computer and the internet have emerged not merely as technological innovations but as the very sinews of modern civilization—catalyzing an

Evidentiary Mechanisms and Forensic Frameworks in the Investigation of Cybercrimes

unprecedented transformation in all sectors of human endeavor, from scientific research and economic productivity to governmental operations and interpersonal communication. These tools have become deeply embedded in the infrastructure of contemporary society, serving simultaneously as repositories of personal and institutional secrets and as the primary medium for instantaneous, borderless interaction. Yet, in a paradoxical twist, these same technologies—once hailed as the harbingers of a new era of enlightenment—have concurrently evolved into potent instruments for perpetrating an entirely new class of criminal offenses: cybercrimes.

Cybercrime, in its myriad and often elusive forms, represents one of the most profound legal and criminological challenges of the digital age. It transcends geographical boundaries, defies traditional notions of territorial jurisdiction, and often leaves behind little or no physical trace. Perpetrators may remain anonymous, concealed behind layers of encryption, proxies, and virtual private networks. Consequently, the act of detecting, investigating, and ultimately prosecuting cyber offenders demands not only sophisticated technological capabilities but also a comprehensive, forward-thinking legal framework capable of adapting to an ever-evolving threat landscape.

A critical component in the war against cybercrime lies in the collection, preservation, and presentation of admissible digital evidence. The legal system must be equipped with robust procedural mechanisms that facilitate the lawful interception of electronic communications, the forensic examination of digital environments, and the expedited preservation of data at risk of obliteration. Without such mechanisms, efforts to bring cybercriminals to justice are doomed to remain inadequate, ineffectual, and, in many cases, purely symbolic.

However, the legislative and prosecutorial response to cybercrime has been uneven and, at times, woefully inadequate. One of the most pressing obstacles that lawmakers continue to face is the classification of cyber offenses. In numerous legal systems, including Algeria's, a significant proportion of cybercrimes remain designated as misdemeanors rather than felonies. This legal categorization, although perhaps justifiable during the embryonic stages of cyber law, now fails to reflect the gravity and transnational ramifications of cyber offenses—many of which are capable of inflicting catastrophic harm on national security, economic stability, and social cohesion.

Fortunately, there has been a discernible shift in both legislative priorities and public perception. The increasing frequency and sophistication of cyber-attacks, coupled with their profound societal impact, have galvanized national and international institutions into action. Specialized cybercrime units have been established within law enforcement agencies and prosecutorial offices, tasked specifically with the digital investigation and prosecution of technology-facilitated offenses. These institutional innovations have significantly elevated the public's awareness of the risks posed by cybercrime and have spurred meaningful legislative reform aimed at fortifying investigative powers while preserving civil liberties.

Going forward, a multifaceted approach is essential. Legislators must continually revise and expand the scope of criminal statutes to encompass emerging modalities of digital criminality. Judges and prosecutors must be trained in the nuances of electronic evidence and digital procedure. Law enforcement agencies must be equipped with state-of-the-art forensic tools and be granted lawful access to encrypted data under judicial supervision. And perhaps most importantly, cross-border cooperation must be intensified through mutual legal assistance treaties and participation in international frameworks such as the Budapest Convention on Cybercrime.

In summation, the fight against cybercrime is not merely a matter of national interest but a global imperative. It demands vigilance, innovation, and above all, a legal consciousness attuned to the

Evidentiary Mechanisms and Forensic Frameworks in the Investigation of Cybercrimes

realities of a world in which crime is increasingly abstract, digitized, and decentralized. By institutionalizing rigorous evidentiary standards and embracing an adaptive, rights-respecting legal architecture, the Algerian legal system—alongside the global community—can rise to meet the formidable challenges of cybercrime in the twenty-first century.

Footnote :

1. Amal Abdel Rahman Youssef Hassan, Modern Scientific Evidence and its Role in Criminal Proof, Master's Thesis in Public Law, Faculty of Law, Middle East University, 2011/2012, p. 41.
2. Amal Abdel Rahman Youssef Hassan, Ibid., p. 42.
3. Mohamed Zarrouk, The Problem of Obtaining Electronic Evidence in Cybercrime, Legal Consultations, posted on 15-05-2020, available at: <https://www.mohamah.net/law>
4. Ben Taleb Linda, Electronic Evidence and its Role in Criminal Proof: A Comparative Study, Doctoral Thesis, Faculty of Law and Political Sciences, Mouloud Mammeri University, TiziOuzou, Algeria, 2019, pp. 47–48.
5. Sara Massaadi, Legitimacy of Digital Media in Criminal Evidence, Algerian Journal of Human Security, Vol. 5, No. 1, January 2020, p. 775.
6. Amal Abdel Rahman Youssef Hassan, op. cit., p. 129.
7. Ibid., pp. 132–133.
8. The unit of measurement "Byte" is the second level unit and consists of 8 bits, where 1 byte = 8 bits. The size or capacity of computer memory is measured by the number of characters it can store. Additionally, data is represented as electronic signals in binary digits (0 or 1). See: Abdulaziz bin Mohammed Al-Obaid, Criminal Liability in Commercial Advertisements: A Foundational Comparative Study, Law and Economics Library, Riyadh, p. 93.
9. Ben Taleb Linda, op. cit., p. 52.
10. Ibid., p. 53.
11. Law No. 04-15 dated 27 Ramadan 1425, corresponding to November 10, 2005, amending and supplementing Ordinance No. 66-156 containing the Penal Code, Official Gazette No. 71, dated November 10, 2004.
12. Law No. 09-04 dated 14 Shaaban 1430, corresponding to August 5, 2009, containing the special rules for the prevention of crimes related to Information and Communication Technology and their suppression, Official Gazette No. 47, dated August 16, 2009.
13. Aisha Ben Gara, The Evidentiary Value of Electronic Evidence in Criminal Proof, New University Press, 2010, p. 101.
14. Law No. 06-22 dated 20/12/2006, containing the Code of Criminal Procedure, Official Gazette No. 84.
15. Search in any residential or non-residential place is allowed at any hour of the day or night with prior authorization from the Public Prosecutor. See: Ben Taleb Linda, op. cit., p. 51.
16. Amal Abdel Rahman Youssef Hassan, op. cit., p. 139.
17. Falah Abdelkader, Seizure and Preservation of Data in Cybercrime, Voice of Law Journal, Vol. 08, No. 01, 2021, p. 179.
18. Jaber Ghanimi, Proving Cybercrimes, published on 13-05-2021, available at: https://www.da5ira.com/2021/05/blog-post_67.html?m=0, accessed on 17-05-2022.
19. Falah Abdelkader, op. cit., p. 180.
20. Falah Abdelkader, Ibid., pp. 180–181.

21. Reziq Mohamed, Procedures of Inspection, Search, and Seizure within the Information System, Master's Thesis in Criminal Law and Criminal Sciences, Faculty of Law and Political Sciences, AkliMohandOulhadj University – Bouira, 2018-2019, p. 46.
22. Samir Chiblaq, The Evidentiary Value of Digital Evidence in Crime Detection, Master's Thesis in Criminal Law and Criminal Sciences, Faculty of Law and Political Sciences, Dr. MoulayTahar University, Saida, 2019-2020, p. 2.
23. ThabetDniyazad, Monitoring Electronic Communications and the Right to Privacy in Algerian Law, Journal of Social and Human Sciences, Vol. 5, No. 1, 2012, p. 207.
24. Reziq Mohamed, op. cit., p. 41.
25. Ibid., p. 42.
26. Ibid., p. 43.
27. Moulek Jamila, Interception of Correspondence, Voice Recording, and Image Capture in Algerian Criminal Procedure Law, Tawasul Journal, Vol. 21, No. 2, 2015, p. 174.
28. AhdadeneSiliya and Laghrib Mohamed Amine, The Impact of Proof by Modern Technological Means on Human Rights, Master's Thesis in Criminal Law and Criminal Sciences, Faculty of Law and Political Sciences, Abdelrahman Mira University, Bejaia, 2017, p. 29.
29. Ibid., p. 29.
30. AbbassiKhawla, Modern Means of Criminal Evidence in Algerian Law, Master's Thesis, Faculty of Law, Mohamed Khider University, Biskra, 2014, p. 42.
31. Article 65 bis 6, paragraph 2, of the Algerian Code of Criminal Procedure.
32. Article 11 of Law No. 09-04 on Special Rules for the Prevention of ICT-Related Crimes and their Suppression.
33. Belabed Aida, Digital Evidence Between the Necessity of Criminal Proof and the Right to Informational Privacy, Scientific Horizons Journal, Vol. 11, No. 1, 2019, p. 141.
34. Ben Zart Asia, Proving Cybercrime in Algerian Legislation, Faculty of Law and Political Sciences, Abdelhamid Ibn Badis University – Mostaganem, 2018-2019, p. 28.
35. The term "service providers" refers to those offering their services to the public at large in the field of information communications, not limited to a specific category of clients through contracts. See: Ben Zart Asia, op. cit., p. 28.
36. Ibid., p. 140.

Bibliography:

A - Books :

1. Abdel Fattah El-Sayfi, Fattouh El-Shazly, Ali El-Kahwaji, *Fundamentals of Criminal Procedures: Pre-trial Procedures, Trial and Appeals*, Al-Jamiaa Publishing House, Beirut; n.d.
2. Ahmed FathiSorour, *Al-Wasit in Criminal Procedure Law, Volume I*, 10th Edition, Dar Al-Nahda Al-Arabiya, Cairo; 2012.
3. Amal Abdel Rahman Youssef Hassan, *Explanation of Criminal Procedure Law*, Egyptian General Book Organization, Cairo; n.d.
4. Raouf Obeid, *Principles of Criminal Procedure in Egyptian Law*, Dar Al-Jeel Publishing, Cairo; 1985.
5. Suleiman Barsh, *Explanation of the Code of Criminal Procedure*, Dar Al-Shehab, Algiers; 1986.
6. GalalTharwat, *Criminal Procedures: The Criminal Case*, University Printing House, Alexandria; 2002.

Evidentiary Mechanisms and Forensic Frameworks in the Investigation of Cybercrimes

7. Aisha Ben Gara, *The Evidentiary Value of Electronic Evidence in Criminal Matters*, New University House, Egypt; 2010.
8. Abdulaziz bin Mohammed Al-Obaid, *Criminal Responsibility in Commercial Advertisements: A Foundational Comparative Study*, Law and Economics Library, Riyadh; n.d.

B – Theses:

1. Meki Ben Sarhan, *The Public Prosecution and the Principle of Discretion in Initiating Public Proceedings*, Doctoral Thesis in Public Law, Faculty of Law and Political Sciences, Saida University; 2019–2020.
2. Ben Taleb Linda, *Electronic Evidence and Its Role in Criminal Proof: A Comparative Study*, Doctoral Thesis, Faculty of Law and Political Sciences, MouloudMammeri University, TiziOuzou, Algeria; 2019.
3. Reziq Mohamed, *Inspection, Search, and Seizure Procedures in the Information System*, Master's Thesis in Criminal Law and Criminal Sciences, Faculty of Law, AkliMohandOulhadj University, Bouira; 2018–2019.
4. Samir Chablaq, *The Probative Value of Digital Evidence in Crime Detection*, Master's Thesis in Criminal Law and Criminal Sciences, Faculty of Law, MoulayTahar University, Saida; 2019–2020.
5. SiliyaIhdadan and Mohamed Amin Lghreib, *The Impact of Modern Technological Means of Proof on Human Rights*, Master's Thesis in Criminal Law and Criminal Sciences, Faculty of Law, Abderrahmane Mira University, Bejaia; 2017.
6. KhawlaAbbassi, *Modern Means of Criminal Evidence in Algerian Law*, Master's Thesis, Faculty of Law, Mohamed Khider University, Biskra; 2014.
7. Ben Zert Asia, *Proof of Information Crime in Algerian Legislation*, Master's Thesis, Faculty of Law, Abdelhamid Ibn Badis University, Mostaganem; 2018–2019.
8. FalahAbdelkader, *Seizure and Preservation of Data in Cybercrime*, Master's Thesis; 2021.

C - Journal Articles:

1. Dreesi Jamal, *The Public Prosecutor's Discretion Regarding Investigative Results Without Referring to the Judge*, Annals of the University of Algiers 1, Vol. 37, No. 2, June; 2023.
2. Sara Messaadi, *Legitimacy of Digital Media in Criminal Evidence*, Algerian Journal for Human Security, Vol. 5, No. 1, January; 2020.
3. ThabetDanyazad, *Monitoring Electronic Communications and the Right to Privacy in Algerian Law*, Journal of Social and Human Sciences, Vol. 5, No. 1; 2012.
4. Jamila Mehlek, *Interception of Correspondence, Voice Recording, and Image Capture in Algerian Criminal Procedure Law*, Journal of Communication, Vol. 21, No. 2; 2015.
5. AqabLarzak, *Legal Provisions of Criminal Mediation in Algerian Legislation*, Law Voice Journal, University of KhemisMiliana, Vol. 6, No. 2; November 2019.
6. Belabed Aida, *Digital Evidence between the Imperative of Criminal Proof and the Right to Information Privacy*, AfaqIlmiya Journal, Vol. 11, No. 1; 2019.

D - Legal Texts and Official Documents:

1. Law No. 04-15 of November 10, 2004, amending and supplementing Ordinance No. 66-156 on the Penal Code, Official Gazette No. 71, November 10, 2004.
2. Law No. 09-04 of August 5, 2009, on Special Rules for the Prevention and Fight Against ICT-related Crimes, Official Gazette No. 47, August 16, 2009.

Evidentiary Mechanisms and Forensic Frameworks in the Investigation of Cybercrimes

3. Law No. 06-22 of December 20, 2006, amending the Criminal Procedure Code, Official Gazette No. 84.
4. Law No. 15-12 of July 15, 2015, on the Protection of the Child, Official Gazette No. 39, July 19, 2015.
5. Article 65 bis 6, paragraph 2 of the Algerian Code of Criminal Procedure.
6. Article 11 of Law No. 09-04 on the Prevention and Fight Against ICT-related Crimes.

E - Websites:

1. Mohamed Zarrouk, *The Problem of Obtaining Electronic Evidence in Cybercrime*, available at: <https://www.mohamah.net/law> (consulted on 15/05/2020).
2. JaberGhoneimi, *Proving Electronic Crimes*, available at: https://www.da5ira.com/2021/05/blog-post_67.html?m=0 (consulted on 17/05/2022).