MAPAN-JOURNAL ,
Publisher: METROLOGY SOC INDIA , NPL PREMISES,
Address: DR K S KRISHNAN MARG, NEW DELHI, INDIA,
ISSN / eISSN:0970-3950 / 0974-9853,
Volume 25-Issue 1-(2025)
https://doi-001.org/1025/17670338533134

Challenges in Proving Electronic Evidence in Cybercrime

Dr. Aouf slimane

Laboratory of Law and Society

Ahmed Draia University of Adrar, Algeria

aoufslimane84@gmail.com

Dr. Ayoub Toumi Lahreche

Laboratory of Law and Political Sciences

Amar Telidji University, Laghouat, Algeria

a.lahreche@lagh-univ.dz

Received: 26/01/2025

Accepted:18/06/2025

Published: 14/12/2025

Abstract:

Information technology has profoundly influenced the nature of crimes associated with it and, in particular, has markedly affected the procedures for their investigation and prosecution. This has led to the emergence of challenges previously unknown to criminal law in both its substantive and procedural dimensions. At the procedural level, the cornerstone of providing cybercrimes lies in electronic evidence, which traditional procedures are incapable of obtaining. Consequently, it is necessary to address the issue of extracting an incriminating proof capable of establishing the offence, given that such evidence possesses an inherent specificity that distinguishes it from conventional forms of proof.

Keywords: cybercrimes; challenges; electronic evidence; virtual environment.

Introduction:

Recent developments in information and communication technology have affected the proof and establishment of criminal evidence in relation to the crimes associated therewith, as traditional forms of evidence have become incapable of proving this modern type of offense. This is because offenders employ highly sophisticated means and methods that enable them to conceal their conduct within a very short time, all within an immaterial environment.[1] This has weakened the probative force of traditional, well-known forms of evidence in establishing guilt. All this, and more, has constituted a compelling reason to seek alternative means and methods compatible with the particular nature of cybercrimes.

The difficulties encountered in acquiring electronic evidence in the virtual environment are among the most significant obstacles. Even if the legislator intervenes by amending procedural provisions pursuant to Law No. 155/66[2] and Law No. 04/09,[3] this does not alter the situation in the face of such technological development unless it is matched by other model solutions aimed at eliminating or reducing the difficulties encountered. This is a matter of paramount importance in confronting and curbing this dangerous type of crime.

Electronic evidence possesses a distinctive and particular nature owing to its technical, intangible, and imperceptible form, in addition to the specific nature of the crime from which it arises. This distinctiveness has, in turn, affected the procedures and methods for obtaining it so that reliance on traditional methods is no longer sufficient to acquire it.[4] Even if it were assumed that the rules governing them had been amended, such an assumption would be illogical unless supported by the technology itself, namely, automated information processing in the collection and extraction of electronic evidence. Accordingly, the problem this study seeks to address is as follows: What are the most significant challenges to the acquisition of electronic evidence?

This question may be addressed through the following axes:

---

[1] El Modhaki, Hanan Reihan Moubarak, *Cybercrimes: A Comparative Study* (Beirut: Al-Halabi Legal Publications, 2014), 41.
[2] Algeria, *Ordinance No. 02/15 of 23 July 2015 Amending and Supplementing Ordinance No. 155/66 of 8 June 1966 Containing the Code of Criminal Procedure*.
[3] Algeria, *Law No. 04/09 Concerning Special Rules for the Prevention of, and the Fight against, Crimes Related to Information and Communication Technologies*, Official Gazette of the People's Democratic Republic of Algeria, no. 47 (2009).
[4] Mamdouh, Abdelhamid Abdelmottaleb, *Digital Criminal Search and Investigation in Computer and internet Crimes* (Cairo: Dar Al Kotob Al Qanounia, 2006), 88.

The first axis: electronic challenges.

The second axis: human challenges.

The First Axis: Electronic Challenges

The nature of evidence is shaped by the nature of the crime from which it arises, for evidence is an effect produced by, or a fact emanating from, the committed offence. Consequently, the difficulties inherent in electronic evidence stem from the internal problems associated with it, given that it results from crimes of a special and distinctive character, which negatively affect the procedures for obtaining and extracting it.

First: The Dynamic Characteristic of Electronic Evidence:

An exceptionally rapid dynamic quality characterises electronic evidence, as it is transmitted through communications networks from one location to another at varying times; it is therefore transboundary, crossing national borders. In other words, information may be stored abroad on servers via remote communication networks. This matter raises numerous problems that may impede the adoption of appropriate procedures for securing and investigating electronic evidence.[5] Because doing so requires action beyond the state's territorial limits, that is, within another state in which the offense, or part of it, was committed. This conflicts with state sovereignty. The problem becomes particularly apparent when search measures are undertaken to secure evidence in such offences, where an automated data-processing system is connected to other systems outside the state, and the search for those systems is necessary to uncover the offense. This necessitates the authorisation of the state within whose territory the search and investigation will be conducted.[6]

In addition, electronic evidence may be modified or erased. Cybercrimes occur within a nontraditional environment, that is, outside the material and tangible framework; their constituent elements arise within the environment of computers and the internet. This is reflected in the evidence they produce, which becomes invisible, thereby rendering its concealment and erasure, whether in whole or in part, or its alteration by the perpetrator extremely easy and capable of being accomplished within a very short time. For example, a user who controls information may employ

[5] Moussa, Mostapha Mohamed, *Criminal Investigation in Electronic Crimes* (Cairo: Police Press, 2008), 213.
[6] Moussa, Mostapha Mohamed, *ibid*., 213.

an information system to erase that information, which constitutes the subject of criminal inquiry, thereby destroying all evidence.[7]

Second: The Invisible Character of Electronic Evidence:

Among the most significant difficulties confronting electronic evidence and those that give rise to numerous problems in its extraction are its invisible and intangible nature. Cybercrimes do not produce fingerprints, footprints, or blood, as in traditional crimes; instead, they give rise only to digital vibrations and impulses constituted within a virtual world that do not disclose a particular identity.[8]Moreover, there is a mixed character resulting from the absence of inherent differentiation within digital storage. The intermingling of the criminal file, which constitutes the subject of electronic criminal evidence, with an innocent file is a plausible occurrence within the storage environment of the virtual world. For example, log files containing an enormous amount of information beneficial to criminal investigation and inquiry pose substantial difficulty for collection, as they are typically intermingled with other information belonging to innocent computer users.[9]

Third: The Encrypted Character of Electronic Evidence:

Crimes committed in the virtual world have produced an offender of a particular nature, namely, the cybercriminal, who exploits his technical and professional skills to attack automated data-processing systems by establishing a security barrier around his unlawful acts prior to committing them so as not to fall within the ambit of punishment. To that end, he relies on restricting, encoding, and encrypting information stored electronically or transmitted via communications networks through constraints that render it impossible for others to access. This amplifies the difficulty of applying procedural rules that enable the extraction of incriminating evidence, thereby constituting an obstacle to investigative and inquiry authorities.[10]

The second axis: Human difficulties

First: Insufficient knowledge and expertise among competent authorities in technical matters:

---

[7] Mamdouh, Khaled Ibrahim, *Cybercrimes* (Cairo: Dar Al Fikr Al Jami'i, 2009), 304.
[8] Mamdouh, Abdelhamid Abdelmottaleb, *ibid.*, 95.
[9] Moussa, Mostapha Mohamed, *Criminal Methods Using Digital Technology: A Comparative Study* (Cairo: Dar Al Kotob Al Qanounia, 2005), 102.
[10] Mamdouh, Khaled Ibrahim, *ibid.*, 309.

A lack of knowledge on the part of the competent authorities regarding the technical and specialist aspects of cybercrimes constitutes one of the obstacles that stand in the way of obtaining electronic evidence, indeed, among the most significant, given the important role played by both judicial and security bodies in investigating crimes and identifying their perpetrators. Accordingly, if, in addition to limited technical expertise, we also face unfamiliarity with handling electronic evidence, we are confronted with a predicament beyond mere acquisition of electronic evidence.[11]

The European Convention on Cybercrime, the conference in Paris titled "Police and the internet," and the Sixth International Conference on Cybercrime held in Egypt have called for the establishment of specialised units to combat technology-related crime.[12]

Many states have responded to this call. Among Western states, the United States established such capacities within the Federal Bureau of Investigation; Spain created the Central Investigations Unit, which is concerned with information technology crimes; and France established several specialised and nonspecialised units and centres within the police and gendarmerie to combat this form of criminality. Among Arab states, Egypt established an administration to combat computer crimes and information networks; Jordan created a special division within the Public Security Directorate tasked with addressing information technology crimes; and Algeria established the National Body for the Prevention of Crimes Related to Information and Communication Technologies.[13]

Second, the difficulty of identifying the perpetrator of a cybercrime is as follows:

Among the most significant human-related difficulties that constitute a stumbling block to the acceptance of electronic evidence is the difficulty of determining the identity of the perpetrator of a cybercrime or its trustworthy source and, in particular, its location. This matter was raised at the International Conference on Computer Crime held in Norway, and it is also among the most prominent problems confronting efforts to combat criminality in the networked world, as stated in the Explanatory Report to the Budapest Convention.[14]

---

[11] Awad, El Hadj Ali Ahmed, and Abd El Amir Khalaf Hussein, *Information Security and Encryption Technologies* (Amman: Dar Al Hamed for Publishing and Distribution, 2004), 210.
[12] Sidi Mohamed El Bachir, *The Role of Digital Evidence in Proving Cybercrimes* (Master's thesis, Naif Arab University for Security Sciences, Riyadh, 2010), 81.
[13] El Hamdani, Bochra Hussein, *Electronic Piracy: Weapons of Modern Warfare* (Amman: Dar Osama for Publishing and Distribution, 2014), 91.
[14] El Halabi, Khaled Ayad, *Procedures of Investigation and Inquiry in Computer and internet Crimes* (Beirut: Dar Al Thaqafa for Publishing and Distribution, 2011), 236.

Even if it is possible to identify the system, namely, the computer, server, host, and networks through which the offense was committed, what is referred to in technical systems as the “IP,” which denotes a number that specifies the identity of the computer connected to the internet and used in committing offences against automated data-processing systems, this number is not standardised worldwide. Only a minority of Arab states employ it, excluding others. This is because the credibility of internet identity via the "IP" address is weak, particularly given that each internet identity line may overlap with multiple identities that may vary among internet users who share the same internet service provider. For example, any person online in Algeria has a specific digital identity; however, if transmission is interrupted and the person reconnects to the internet, the previous identity will no longer belong to them but to someone else. Accordingly, he may appear under a different "IP" identity, making it challenging to identify the offender. The matter becomes even more difficult when the computer is in a semipublic place, such as a company, office, institution, or internet café, where any individual may interact with networks, including the offender who uses them to commit his crimes. This makes it challenging to identify the perpetrator, as the offender may move to multiple cafés in a single day, which in turn makes it difficult to obtain evidence regularly because such cafés reconfigure their devices. In addition, it is possible to carry information under "IP" addresses that are not real or falsified so that it appears that the information originated from a particular processor. In reality, it originated from another computer.[15]

"ADSL" technology, or what is termed high-speed internet, has likewise not been spared by criminals, who have used it to implement their criminal schemes alongside other persons on a single device through a line distributor, making it difficult to identify them.[16]

The emergence of wireless internet has made it difficult to detect the perpetrator of a cybercrime owing to the ease of moving to several locations within a single day. The acts of concealment have further increased the difficulty of navigating the network, as hackers have exploited them; indeed, the designers of destructive viruses have launched them worldwide through such sites, a development that has become a grave phenomenon.[17]

---

[15] Sidi Mohamed El Bachir, *ibid.*, 80.
[16] Othmani, Leila, “Obtaining Electronic Evidence within the Framework of the (TCP/IP) Protocol: A Comparative Study,” *Sawt al-Qanoun* (University of Khemis Miliana) 7, no. 3 (2021): 593.
[17] Ezzaydi, Walid, *Hacking the internet and the Computer* (Amman: Dar Osama for Publishing and Distribution, 2003), 66.

Third, the Refusal of Victims of Cybercrimes to Report Them upon Discovery:

With reference to the Algerian Penal Code, which provides that every citizen has the right to report so long as the offense is not among those requiring a complaint or request from the body designated by law, reality has shown the contrary, as we find a paucity indeed, an absence of security and judicial cases relating to cybercrimes. This is attributable to their distinctive nature, which makes them difficult to detect: they are unknown and concealed, operate in technical environments, and leave no trace. Even if they are discovered, in most cases, the victim conceals them rather than calling the police out of fear that vulnerabilities in their system will be uncovered. This increases the difficulty not only in detecting such crimes but also in studying the phenomenon as a whole.[18]

Both the Fifteenth International Congress of the General Association of Penal Law and the Eighth Resolution concerning the prevention of crime and the treatment of prisoners, issued by the United Nations, recommended encouraging victims and other users of information technology to report the crimes to which they are subjected.

Notably, among the proposals advanced to induce victims to cooperate with authorities in the United States, some call for legal provisions related to information-technology crimes to impose an obligation upon employees of the victim entity to report any information they receive concerning the occurrence of such crimes, with a penalty prescribed for breach of that obligation.[19]

Conclusion:

In conclusion, the difficulty of proving cybercrimes stems from the nature of the evidence derived from them, as well as the need for scientific and technical knowledge that may not be available to competent authorities. Consequently, these challenges often remain difficult to resolve in the absence of a clear strategy for addressing this category of crimes and their perpetrators, particularly in states whose legislation has not been amended to keep pace with technological development.

Bibliography

Primary Sources

[18] El Hamdani, Bochra Hussein, *ibid.*, 84.
[19] Belhadi, Hamid, "The Evidential Value of Digital Evidence in Criminal Proof," *Journal of Legal and Political Research and Studies* (University of Blida 2) 9, no. 1 (2019): 24.

Algeria. *Law No. 04/09 Concerning Special Rules for the Prevention of and Fight against Crimes Related to Information and Communication Technologies*. Official Gazette of the People's Democratic Republic of Algeria, no. 47, 2009.

Algeria. *Ordinance No. 02/15 of 23 July 2015 Amending and Supplementing Ordinance No. 155/66 of 8 June 1966 Containing the Code of Criminal Procedure*.

Secondary Sources

Books

El Hamdani, Bochra Hussein. *Electronic Piracy: Weapons of Modern Warfare*. Amman: Dar Osama for Publishing and Distribution, 2014.

Ezzaydi, Walid. *Hacking the internet and the Computer*. Amman: Dar Osama for Publishing and Distribution, 2003.

El Modhaki, Hanan Reihan Moubarak. *Cybercrimes: A Comparative Study*. Beirut: Al-Halabi Legal Publications, 2014.

El Halabi, Khaled Ayad. *Procedures of Investigation and Inquiry in Computer and internet Crimes*. Beirut: Dar Al Thaqafa for Publishing and Distribution, 2011.

Awad, El Hadj Ali Ahmed, and Abd El Amir Khalaf Hussein. *Information Security and Encryption Technologies*. Amman: Dar Al Hamed for Publishing and Distribution, 2004.

Mamdouh, Khaled Ibrahim. *Cybercrimes*. Cairo: Dar Al Fikr Al Jami'i, 2009.

Mamdouh, Abdelhamid Abdelmottaleb. *Digital Criminal Search and Investigation in Computer and internet Crimes*. Cairo: Dar Al Kotob Al Qanounia, 2006.

Moussa, Mostapha Mohamed. *Criminal Methods Using Digital Technology: A Comparative Study*. Cairo: Dar Al Kotob Al Qanounia, 2005.

Moussa, Mostapha Mohamed. *Criminal Investigation in Electronic Crimes*. Cairo: Police Press, 2008.

Thesis

Sidi Mohamed El Bachir. “The Role of Digital Evidence in Proving Cybercrimes.” Master’s thesis, Naif Arab University for Security Sciences, Riyadh, 2010.

Journal Articles

Belhadi, Hamid. “The Evidential Value of Digital Evidence in Criminal Proof.” *Journal of Legal and Political Research and Studies* (University of Blida 2) 9, no. 1, 2019.

Othmani, Leila. “Obtaining Electronic Evidence within the Framework of the (TCP/IP) Protocol: A Comparative Study.” *Sawt al-Qanoun* (University of Khemis Miliana) 7, no. 3 2021.