Ziglôbitha,
Revue des **A**rts, **L**inguistique,
Littérature & **C**ivilisations
Université Peleforo Gon Coulibaly - Korhogo

Local Legislation in Combating Cybercrimes: "Algeria as a Model"

Sakhri NADJIA
University of Oran 2- Algeria
nadjiasamir992@gmail.com

Remli FAHIM
University of Blida 2 -Algeria
f.remli@univ-blida2.dz

Bensalah ABDALLAH
University of Algiers 3 - Algeria
abdallahbensalah2@gmail.com

Résumé : Il ne fait aucun doute que la cybercriminalité est considérée comme l'un des crimes les plus avancés et les plus complexes en raison de sa dépendance à l'égard du renseignement technique et informationnel, ce qui a rendu de nombreux pays impuissants et largement incapables de l'affronter et de la combattre en raison de sa spécificité et de son caractère avancé. Dans cet article, la cybercriminalité sera étudiée et détaillée en détail. Cet aspect est obtenu en combinant les aspects conceptuels et originaux de ce type de criminalité tout en suivant un certain nombre de législations locales, en se concentrant sur l'étude du cas algérien, qui œuvre à couvrir tous les secrets des délits électroniques, en essayant ainsi d'explorer leurs forces et leurs faiblesses et ainsi tester l'étendue de leur efficience et de leur efficacité dans la détection de ces délits. Ces délits sont réduits, puis des recommandations sont formulées pour combler le vide juridique existant dans la législation locale et déterminer les les chemins qu'il faudra suivre à l'avenir pour les éliminer.
Mots clés : Législation Local ; Crimes Electroniques ; Algérie ; Constitution Algérienné.

Abstract: There is no doubt that cybercrime is considered one of the most advanced and complex crimes due to its dependence on technical and informational intelligence, which has made many countries helpless and largely unable to confront and combat it due to its specificity and advanced nature. In this article, cybercrime will be studied and detailed in detail. This aspect is achieved by combining the conceptual and original aspects of this type of crime while following a number of local legislations, focusing on the study of the Algerian case, which works to cover all the secrets of electronic crimes, thus trying to explore their strengths and weaknesses and thus test the extent of their efficiency and effectiveness in detecting these crimes. These crimes are reduced, then recommendations are made to fill the legal gap existing in local legislation and determine the paths that will have to be followed in the future to eliminate them.

Keywords: Local Legislation; Electronic Crimes; Algeria; Algerian Constitution.

Introduction:

The change in human interaction spaces and the rapid, unorganized shift to the virtual world have led to the emergence of a new type of silent crime with negative implications for the security of states and societies. Cybercrimes have emerged as a novel type of crime aimed at undermining individuals' digital privacy and the informational security of countries and governments that have transferred many of their administrations and fields of work to the information space as part of digitizing vital sectors related to the economy and local administration. However, the existing digital gaps and their exploitation by cybercriminals have made the cybersecurity of these countries and societies subject to constant threat. This is accompanied by incomplete legal and legislative follow-up arising from the novelty of the phenomenon and the difficulty of investigation it entails. In this context, Algeria, like many other countries, has rushed to establish a national legislative framework aimed at containing the phenomenon and mitigating its effects. Many laws related to combating cybercrime have been enacted, such as Section 7 bis of the Penal Code No. 04-15, titled 'Infringement of Automated Data Processing Systems.'

0.1. Research Problem:

As part of Algeria's national strategy to achieve cybersecurity and defense, efforts have been made to establish a comprehensive legislative framework that addresses the phenomenon of cybercrime in terms of its elements, forms, and methods of investigation. This is a step toward legally and practically containing it by identifying and deterring perpetrators. This leads us to pose the following research question:

How has the Algerian legislator dealt with the phenomenon of cybercrime?

0.2. Research Hypothesis:

Cybercrimes require strict legal rules that combine legislative and technical aspects to address the unique nature of these crimes and overcome the challenges faced in investigation and punishment.

0.3. Research Methodology:

To explore the topic of local legislation and cybercrimes, the descriptive-analytical method was employed. This approach allows for a detailed examination of cybercrimes and their characteristics as an initial step toward exploring the local legislation dedicated to addressing them and what distinguishes them in terms of their legal structure and the nature of the materials

they contain, in order to analyze them and determine their strengths and weaknesses.

0.4. Study Importance and Objectives:

Cybercrimes are among the most advanced crimes, relying heavily on technical and informational intelligence. Many governments struggle to keep up with these crimes due to their unique and evolving nature. This study aims to provide research that combines the conceptual and etymological aspects of this type of crime while simultaneously examining various local legislations that attempt to contain it. The study seeks to explore the strengths and weaknesses of these laws and assess their effectiveness in detecting and reducing cybercrimes. The ultimate goal is to reach recommendations that bridge the existing legal gap and identify future courses of action to mitigate these crimes.

1. Cybercrime – "A Conceptual Introduction"

1.1. Definition of Cybercrime:

Cybercrime encompasses a variety of sub-crimes that collectively form the broader concept. Therefore, attempting to define the term requires examining and identifying these individual crimes to arrive at an accurate definition. This will be addressed through the following points:

- **Computer Crimes**: The control over computers has led to the emergence of a new type of crime committed using these devices, aiming to cause material and moral harm to others. Several definitions have been proposed for this type of crime. Some define computer crimes as any illegal act where the computer is used as a tool or subject of the crime, or as an act punishable by law committed by someone with sufficient knowledge of computer technology. Others describe it as a non-traditional crime that emerged with the advent of computers and networks, resulting in material and moral harm to others[1]. Thus, computer crimes involve attacks on computer systems, whether on their physical components, such as input and output units, or their intangible components, such as information and data stored within them.[2]

- **Internet Crimes:**

[1] Mohsen Ben Suleiman Al-Khalifa, *Computer Crimes and Their Penalties in Jurisprudence and Law* (Crimes of Copying Computer Programs and Selling Them, Producing and Spreading Viruses), Riyadh: King Naif University for Security Sciences, 1423 AH, pp. 42-43.

[2] Ibrahim Ramadan Ibrahim Al-Attaya, *Cybercrime and Ways to Address It in Islamic Law and International Systems* (An Analytical and Applied Study), Volume 30, Issue 2, April 2015, p. 371.

The European Convention on Cybercrime 2001 defines them as "all illegal or unlawful activities associated with computer systems and the use of the internet."[3]

Internet crimes are those that aim to disrupt, deface, or modify websites, or involve unauthorized access to restricted areas. They also include using false addresses to access information networks, spreading viruses, and sending various types of emails, including those that harm individuals' dignity or promote illegal materials or activities.

- **Information Network Crimes:**

These crimes involve any unlawful act affecting documents or texts available on a network. Examples include violations of intellectual property rights related to software, artistic, literary, and scientific productions. Such crimes are committed through information networks, requiring an internet connection and the use of a computer to access or modify databases.[4]

Since computers serve as a link between all these crimes categorized under cybercrime, it is essential to clarify the methods through which computers are used to commit legal violations in the digital world. Below are the main ways in which computers are employed in various criminal activities.

1. Computer Virus:

A computer virus is a harmful software that infects programs, information, or the computer itself, potentially causing damage that can completely or partially disable the device. Similar to a biological virus, it spreads from one device to another when devices are connected through a network, or via linked communications, or through a disk that carries or is infected with the virus. The virus spreads electronically and can lead to the destruction or loss of the information stored on the infected device.

2. Computer Fraud:

Computer fraud refers to any deceitful actions involving information where a criminal aims to achieve financial gain through the use of a computer. This can include tactics such as withdrawing money from bank accounts through fraudulent maneuvers or deceiving individuals or companies to seize their funds.

[3] Hatem Ahmed Mohamed Batikh, *The Evolution of Legislative Policy in the Field of Combating Information Technology Crimes*, *Journal of Legal and Economic Studies*, Volume 01, Issue 2, June Supplement 2021, p. 15.

[4] Ibrahim Ramadan Ibrahim Al-Attaya, *Op. Cit.*, p. 371.

3. Information Theft and Espionage:

Theft in the computer realm involves stealing information and programs stored on a computer or disk.[5] This represents violations of the confidentiality of personal data and its disclosure, often through eavesdropping and spying on computer systems and intercepting electronic communications. Typically, this is accomplished by installing spyware, which is designed to collect data from a computer or device and redirect it to another party without the user's consent or knowledge. This usually involves gathering confidential information such as passwords, PIN codes, credit card numbers, monitoring keystrokes, tracking browsing habits, and collecting email addresses.[6]

Therefore, the various actions outlined above are essentially components of cybercrime, which relies on modern technology, the internet, computers, information networks, technical equipment, and knowledge of the virtual world. Cybercrime involves using these tools to manipulate devices and data unlawfully, without legal authorization to access, handle, or alter private information, or to distort it with the intent of causing material and moral harm to the victim, whether an institution or an individual.

2. Characteristics of Cybercrime:

Based on the definitions provided above related to cybercrimes, several defining elements can be inferred that essentially characterize this type of crime.

- **Transnational Crime**:

  One of the key characteristics of cybercrimes is that they transcend the geographical borders of a single country due to their connection with the internet and information technology. They can affect multiple countries simultaneously because of their rapid execution.

- **Difficulty in Proving and Detecting Cybercrime**:

  Cybercrimes fall under the category of emerging crimes, which are difficult to detect and prove for the following reasons:

. Crimes committed against or through information systems and networks rarely result in tangible physical effects.

. The presence of a large number of individuals at the crime scene between the commission of the crime and its discovery can lead to changes, damage, or

[5] *Computer Crimes*, *Army Magazine*, Issue 232, 2004, accessed at the following website: https://www.lebarmy.gov.lb/ar/content/%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D9%83%D9%88%D9%85%D8%A8%D9%8A%D9%88%D8%AA%D8%B1

[6] What is Spyware? - Definition, on the website: https://me.kaspersky.com/resource-center/threats/spyware , accessed on 20/10/2020 at 7:48.

tampering with physical evidence, or even the deletion of some evidence, raising doubts about the reliability of the evidence collected for examination.
. The perpetrator's ability to manipulate or erase data remotely by accessing the system through a terminal unit.[7]

- **Crimes Requiring a Computer and Technical Knowledge:**

A computer is both a primary object of cybercrime and a tool used to commit the crime. It represents a protected asset while also being a means to perpetrate the offense. In cybercrimes, the perpetrator can be an individual acting on their own, aiming to achieve personal gain through crimes committed against data processing systems. However, it is common for individuals to commit criminal acts not for their own benefit but on behalf of a legal entity, such as a company operating in the field of information technology or another sector.

- **Soft Crimes**:

Traditional crimes often involve the use of criminal tools and violence, as seen in terrorism, drug trafficking, theft, and armed robbery. In contrast, crimes associated with computers and the internet are characterized as "soft crimes" because they do not require physical violence. Activities such as transferring data from one device to another or electronic theft of bank accounts do not involve physical violence but occur in a quiet and subtle manner.

Thus, cybercrimes rely on intelligence and knowledge, making them difficult for traditional investigators to handle, detect, and provide evidence for. These crimes are marked by their ambiguity. As technological knowledge and individual expertise in using it for criminal purposes advance[8], it becomes increasingly difficult to understand these crimes and to develop immediate laws that align with their specific and evolving characteristics.

3. Local Legislation in Addressing Cybercrime

The rapid and widespread rise of cybercrimes in the Arab world has led its countries to adopt stringent legislative measures to curb the proliferation of these crimes, deter offenders, and restore the rights of victims. Below are the key local legislative contributions aimed at combating all forms of cybercrime.

[7] Maemach Zahia and Ghanem Nassima, *Criminal Evidence in Information Crimes*, Master's thesis in Legal Sciences, University Abderrahmane Mira of Béjaïa, 2013, p. 16.
[8] Samira Maachi, *The Nature of Information Crime*, *Legal Forum Journal*, Issue 7, April 2010, p. 283.

3.1. In Egyptian Legislation:

Although Article 31 of the Egyptian Constitution issued in 2014 explicitly mandates the protection of electronic information and data, stating that "Cybersecurity is an essential part of the economic and national security system, and the state is obligated to take necessary measures to protect it, as regulated by law," there is still no comprehensive criminal legislation specifically addressing cybercrimes. Legislative contributions are limited to certain legal provisions, including but not limited to the following examples:

- **Personal Status Law No. 143 of 1994**: This law regulates, in several of its articles, the criminalization of altering personal status data of citizens recorded on computers or electronic media within the Civil Status Department of the Ministry of Interior through forgery, destruction, or unauthorized access. Articles 72, 74, 75, and 76 of the law outline methods of destroying official recorded information and violating its confidentiality, while also specifying the penalties, such as fines, imprisonment, or hard labor.
- **Intellectual Property Protection Law No. 82 of 2002**: This law contains provisions that protect against literary theft conducted through the internet in some of its articles.
- **Telecommunications Regulation Law of 2003**: This law, particularly in Article 73, outlines unlawful acts that include violations of individuals' informational privacy.[9]
- **Law No. 175 of 2018 on Combating Information Crimes**: Article 25 of this law states, "A penalty of imprisonment for a period of no less than six months, and a fine of no less than fifty thousand Egyptian pounds and not exceeding one hundred thousand Egyptian pounds, or one of these penalties, shall be imposed on anyone who violates any of the principles or family values in Egyptian society, invades the sanctity of private life, sends numerous electronic messages to a specific person without their consent, or publishes through the information network or any means of information technology news, images, or similar materials that violate the privacy of any person without their consent, whether the published information is true or false."[10]

[9] Adel Amer, *Cybercrime Under Egyptian Law*, published on Donia Al-Watan on 11/04/2020, accessed on https://pulpit.alwatanvoice.com/articles/2020/04/11/518932.html on 30/01/2022.
[10] *Official Gazette*, Issue 32 (Supplement C), on August 14, 2018, Article 25, p. 18.

3.2. Cybercrime in Gulf Legislation:

The Gulf countries are among the most affected by the outcomes of cybercrime due to the extensive digitization that governments are implementing across various vital sectors. Additionally, the high standard of living in these countries necessitates a pattern of virtual relationships among members of society. Below are the key Gulf legislations that have addressed cybercrime:

. The Qatari Law No. 14 of 2014, issued on September 15, 2014, defines cybercrime as follows: "Any act that involves the use of an information technology tool, an information system, or the information network in an unlawful manner."

. The Saudi Anti-Cyber Crime Law explicitly defines cybercrime in Paragraph 8 of Article 1 of the system issued by Royal Decree No. M/17 dated 08/03/1428 AH as "any act committed involving the use of a computer or the information network in violation of the provisions of this system."

. The UAE legislator issued Federal Law No. 2/2006 on Combating Information Technology Crimes, which was later repealed by Federal Decree-Law No. 5/2012 on Combating Cybercrimes, as termed by the UAE legislator. This law did not provide a specific definition of cybercrime but rather outlined the actions that fall under it in Articles (02 to 44) of the same law.[11]

It is evident that Arab laws vary in their adaptation to cybercrime, primarily due to the internal conditions of each country, which determine the extent of their integration into the world of technology and their use of information and communication technologies. Additionally, countries are influenced by the ability of individuals to use modern devices and the information network in criminal activities, as well as the degree of their impact on electronic stability. If a country does not fully digitize its vital sectors, its cybersecurity does not become a serious threat, as it has not yet achieved high levels of digital engagement locally and globally. Conversely, countries that have moved towards modernization and digitization have needed deterrent laws that define the types of actions that fall under cybercrime and impose strict penalties to reduce attacks on devices, individuals, and official and private institutions.

[11] Research and Studies Center, Sultan Qaboos Academy for Police Sciences, *Cybercrime in the Gulf Society and How to Address It*, paper submitted for the Prince Nayef Security Research Award 2015, published by the Gulf Cooperation Council, 2016, pp. 22-23.

4. The Reality of Cybercrime in Algeria and Legal Mechanisms for Combating It

The scope of cybercrime in Algeria has expanded alongside the widespread use of internet-connected technology in Algerian society. Estimates indicate that cybercrime has developed significantly in recent years, with cases increasing from 18 in 2008 to 102 in 2013, and reaching 1,652 cases in 2019.[12]

To curb these crimes, the Algerian legislator adopted the term "affecting automated data processing systems" to refer to cybercrime, considering that the information system and its intangible components are the primary area for this type of crime. The legislator has worked to keep pace with the developments of the information revolution by introducing several legislative provisions specific to this criminal pattern, which will be detailed in the following points:

4.1. Criminalizing Cyber Attacks Under Algerian Penal Code:

Initially, the Algerian legislator sought to address cybercrimes by amending the Penal Code through Law No. 04-15 dated November 10, 2004, which supplements Ordinance No. 66-156 containing the Penal Code. This amendment introduced Section 7 bis titled "Affecting Automated Data Processing Systems" through Articles 394 bis and 394 bis 7.

In general, the criminalized acts under this law can be summarized as follows:

- Unauthorized Access and Presence in Automated Data Processing Systems: The law stipulates: "Anyone who enters or remains in whole or in part of an automated data processing system through deception or attempts to do so shall be punished with imprisonment for three months to one year and a fine ranging from 50,000 to 100,000. The penalty is doubled if such actions result in the deletion or alteration of data in the system, and if these actions lead to the destruction of the system's operational functionality."
- Deliberate attacks on automated data processing systems
- Deliberate attacks on the integrity of data within the system

In 2006, the Algerian legislator introduced another amendment to the Penal Code, Law No. 06-23 dated December 20, 2006, which affected the seventh section bis concerning crimes affecting data processing systems. The amendment

[12] Jouida Bouaraba, *National Gendarmerie in the Face of Cybercrime*, translated by Mohamed Maïouf, *Army Magazine*, Issue 685, August 2020, p. 21.

tightened the penalties for these actions without altering the criminal provisions stated in this section of the law.[13]

4.2. Handling Cybercrime Under the Algerian Code of Criminal Procedure

- Establishing specialized criminal courts with expanded jurisdiction that may extend their jurisdiction to consider crimes affecting data processing systems (Articles 37, 40, 329)
- Extending the territorial jurisdiction of judicial police officers to investigate crimes affecting data processing systems throughout the entire national territory (Article 16).
- The possibility of using special methods in crimes affecting data processing systems, such as intercepting communications made through wired and wireless means, capturing and recording and broadcasting conversations and images of individuals in private places (Articles 65 bis 5 to 65 bis 10).[14]

4.3. Cybercrime in Algerian Special Laws:

Many Algerian special laws address crimes affecting automated data processing systems, such as the Social Security Law concerning unauthorized use of electronic cards, Law No. 15-03 related to modernizing the judiciary, and the Law on Preventing Crimes Connected to Information and Communication Technology, which we will detail in the following points:

- This law was enacted to address the existing legislative gaps in combating electronic crime. The Algerian legislator worked to issue a new law to tackle all crimes resulting from the unlawful use of the internet and information and communication technology. One of the key features of this law is that it supports the Criminal Procedure Code and outlines preventive measures that allow for early detection of potential attacks and rapid intervention to identify their sources and perpetrators.
- Search and Seizure of Information: This law ensures, through its fifth and sixth articles, the possibility for specialized authorities to access the information system or parts of it, even remotely. It also allows for the assistance of specialized foreign authorities to obtain data sought in an information system located in another country. Additionally, the law permits investigators to duplicate data

[13] For more on this part, see: Dawad Wessila, *Cybercrime in Light of the Algerian Penal Code*, Master's thesis, Abdelhamid Ben Badis University, Mostaganem, 2019, and Saida Bouznoun, *Combating Cybercrime in Algerian Legislation*, Journal of Human Sciences, Volume B, Issue 52.

[14] Hanane Meskine, "The Reality of Combating Cybercrime and Its Legislative Trends in Algeria," *Academic Journal of Legal and Political Research*, Vol. 04, No. 01, 2020, pp. 619-620.

under investigation if it proves useful for uncovering crimes or identifying perpetrators.

- The law established an agency responsible for preventing and combating electronic crimes: the National Authority for the Prevention of Information and Communication Crimes. This agency is tasked with several duties, including monitoring electronic communications related to crime and protecting the obtained data from any destruction or tampering.[15]

To support these legislations and in line with the nature of such complex crimes, several specialized institutions have been established, including the Cybercrime Combat Center under the Algerian National Gendarmerie, the Cyber Defense and System Security Monitoring Department within the National People's Army. In August 2021, a new judicial pole was created to follow up and combat cybercrimes: the Digital Evidence Department of the National Security.[16]

Thus, it becomes clear that combating the complex nature of cybercrime requires not only legal frameworks that define penalties for offenders but also a comprehensive approach that addresses all the technical elements associated with these crimes. This should enable the establishment of specialized institutions that assist in prevention, early warning, and continuous awareness of the risks posed to individual and national security.

Conclusion:

Based on what was covered in the research, the following results were reached:

- Cybercrimes are considered sophisticated crimes resistant to all forms of identification, investigation, and evidence. These crimes heavily rely on individuals' ability to navigate the complexities of the digital world, making it difficult to track them and search for traces that can be concealed. Thus, it is challenging to develop dynamic legislation that aligns with the evolving nature of these crimes, especially since the creation of laws often requires multiple stages and the assistance of technical experts who help identify the possible forms of attacks on devices and individuals electronically.
- The types of cybercrime are numerous, and currently, the most challenging ones are related to the safety of societal values, identities, and religions. The

[15] For more details, see: Mourad Mechouch, "Cybercrime in Light of the Penal Code and the Law on Crimes Related to Information and Communication Crimes," *Journal of Law*, Vol. 09, Issue 01, 2020.

[16] For more information, see: *Monthly Magazine of the National People's Army*, Issue 701, December 2021, File: New Generation Wars, pages 37 to 48, available at: https://www.mdn.dz/site_principal/sommaire/revues/images/EldjeichDec2021Ar.pdf

use of the internet and social networks has become a means to infiltrate societies and undermine their cohesive structures by launching campaigns against national symbols, flooding communities with false information, deceptive propaganda, and harmful rumors. All these fall under what is known in strategic literature as psychological warfare, a method of cyber warfare aimed at threatening the societal security of states without direct confrontation. This means that cybercrimes may include non-material objectives and are supported by entities hostile to the targeted countries.

- Governments may face the issue of interfering with individuals' digital privacy rights, which are protected under international law, while organizing legal means for detecting and combating cybercrime. Therefore, it is necessary for them to consider all legal aspects that help avoid such interference.

The legal framework established by the Algerian legislator for cybercrime is an important framework that keeps pace with the evolving nature of this type of crime and achieves the necessary flexibility to address it. However, this does not reduce the possibility of criminals evading capture due to the nature of the crime, which involves deliberate destruction of information and data and the difficulty in identifying virtual parties. This significantly impedes the investigative processes undertaken by local authorities to uncover these crimes.

Based on this, the following recommendations are provided:

- Work on establishing institutional frameworks with legal independence, consisting of both national and foreign experts trained in law and information technology. These frameworks should be dedicated to developing robust programs with high-level encryption systems that intruders cannot breach, especially concerning networks connected to national infrastructure and the economy. Attacks on these areas represent a form of assault on the state's sovereignty and one of its domains: the informational-cyber domain.
- Develop local legislation and attempt to move away from the static nature of traditional legislative processes. Legislators must include provisions that allow for the rapid amendment of laws, making them flexible in dealing with the rapid advancements in information and communication technology and the associated crimes.
- Work to achieve regional and international coordination regarding the development of local laws by joining relevant agreements and establishing institutions that facilitate the exchange of information during and after investigations, within a collaborative strategy that allows for the benefit of external expertise.

- Achieve the principle of digital sovereignty, which requires the state to exercise control and demonstrate its ability to protect its cyber space from any potential violations.

Bibliographical References :

Al-Khalifa Mohsen Ben Suleiman (1423 AH), Computer Crimes and Their Penalties in Jurisprudence and Law (Crimes of Copying Computer Programs and Selling Them, Producing and Spreading Viruses), Riyadh: King Naif University for Security Sciences.

Al-Attaya Ibrahim Ramadan Ibrahim (2015), Cybercrime and Ways to Address It in Islamic Law and International Systems (An Analytical and Applied Study), Volume 30, Issue 2.

Amer Adel, Cybercrime Under Egyptian Law, published on Donia Al-Watan on 11/04/2020, accessed on https://pulpit.alwatanvoice.com/articles/2020/04/11/518932.html on 30/01/2022 .

Batikh Hatem Ahmed Mohamed (2021), The Evolution of Legislative Policy in the Field of Combating Information Technology Crimes, Journal of Legal and Economic Studies, Volume 01, Issue 2.

Bouaraba Jouida (2020), National Gendarmerie in the Face of Cybercrime, translated by Mohamed Maïouf, Army Magazine, Issue 685.

Bouznoun Saida (2023), Combating Cybercrime in Algerian Legislation, Journal of Human Sciences, Volume B, Issue 52.

Computer Crimes, Army Magazine, Issue 232, 2004, accessed at the following website: https://www.lebarmy.gov.lb/ar/content/%D8%AC%D8%B1%D8%A7%D8%A6%D9%85-%D8%A7%D9%84%D9%83%D9%88%D9%85%D8%A8%D9%8A%D9%88%D8%AA%D8%B1

Dawad Wessila (2019), Cybercrime in Light of the Algerian Penal Code, Master's thesis, Abdelhamid Ben Badis University, Mostaganem.

Maemach Zahia and Ghanem Nassima (2013), Criminal Evidence in Information Crimes, Master's thesis in Legal Sciences, University Abderrahmane Mira of Béjaïa.

Maachi Samira (2010), The Nature of Information Crime, Legal Forum Journal, Issue 7.

Meskine Hanane (2020), "The Reality of Combating Cybercrime and Its Legislative Trends in Algeria," Academic Journal of Legal and Political Research, Vol. 04, No. 01.

Mechouch Mourad (2020), "Cybercrime in Light of the Penal Code and the Law on Crimes Related to Information and Communication Crimes," Journal of Law, Vol. 09, Issue 01.

Monthly Magazine of the National People's Army, Issue 701, December 2021, File: New Generation Wars, available at: https://www.mdn.dz/site_principal/sommaire/revues/images/EldjeichDec2021Ar.pdf

Official Gazette (2018), Issue 32 (Supplement C), on August 14, Article 25.

Research and Studies Center (2016), Sultan Qaboos Academy for Police Sciences, Cybercrime in the Gulf Society and How to Address It, paper submitted for the Prince Nayef Security Research Award 2015, published by the Gulf Cooperation Council.

What is Spyware? - Definition, on the website: https://me.kaspersky.com/resource-center/threats/spyware , accessed on 20/10/2020 at 7:48.