Infitration as a Mechanism for Detecting Cybercrime

Amraoui khadidja*

University Abbas Lagrour.khenchela
Amraoui-khadidja@univ-khenchela.dz

Send Article Date: 04/12 / 2023 Date of acceptance of the article:19/.01 /2024

****

Abstract:

The evolution of society has led to the development of crime and its methods. Scientific and technological progress has contributed to the emergence of crimes characterized by the sharp intelligence of their perpetrators, namely cybercrimes. These crimes are difficult to prove because their perpetrators are characterized by professionalism and the exploitation of modern scientific means.

This is what prompted the Algerian legislator to introduce in Law 06/22 of December 20, 2006, amended and supplemented the Code of Criminal Procedure, a new mechanism for detecting cybercrimes, which is infiltration. This is done through the joining of a judicial police officer or one of the judicial police officers to the criminal group under a false identity to uncover the truth and punish the perpetrators of the crimes, and this within formal and material conditions, and with the permission of the competent judicial authority, represented by the prosecutor or investigating judge who is responsible for giving permission and monitoring the necessity of the principle of integrity or not.

key words: Cybercrimes, infiltration, Conditions for infiltration.

---

* Amraoui Khadidja

Introduction :

Cybercrimes are difficult to detect and identify the physical evidence that incriminates the perpetrator, due to the development of computer crimes, it is necessary to make efforts and keep pace with developments to combat these crimes by keeping pace with the new laws in order to deter those who commit these crimes and to develop an effective strategy to combat these crimes in order to reduce them and control them.

The search and investigation about it in order to prove it has become very difficult for those in charge, due to the inability of traditional search and investigation means to detect these sophisticated crimes, especially as their perpetrators are characterized by professionalism and exploitation of modern scientific means.

From here, all legislations had to change their traditional policy by searching for advanced means to detect this type of information crimes, this is what made the Algerian legislator also search in this field, he included legal rules that expand the jurisdiction of the judiciary, and reinforce the powers and jurisdiction of the judicial police, by putting the infiltration mechanism to confront information crimes.

The importance of this study comes in the fact that infiltration is a mechanism introduced by Law 06/22 amended and supplemented by the Code of Criminal Procedure, to reach the people who commit cybercrimes, through the infiltration of the judicial police officer or assistant inside the criminal group to reach the truth.

From here, the following problem can be raised:

How effective is the infiltration method in detecting cybercrimes?

To answer this problem, we are going on the following plan:

SECTION 1: cybercrimes and infiltration: overview

Second topic: The role of infiltration in detecting cybercrime

Conclusion:

SECTION I : cybercrimes and infiltration: overview

The technological revolution and the resulting information revolution have had a significant impact on the lives of individuals and societies in a positive way. This is due to the increasing use of computers, which come in various forms, such as desktop, laptop, and mobile phones, and are connected to the internet almost all the time.

This has made it possible for individuals to meet their needs, such as learning, health, communication, contracting, and obtaining documents, in a simple way by pressing a button or touching a digital screen, instead of having to travel from one place to another. This is in contrast to the past.

However, these technological developments have also led to the emergence of many negative phenomena, such as the rise of cybercrime. This crime has attracted a new category of criminals who have used this technology - information systems - as a tool for crime in a contemporary form, in a way that is not understood by traditional crime, through its accelerated pace, in terms of the speed of its development, the areas it will target, and its effects. This has led researchers in various fields, including technical informatics, social, and legal, to conduct contemporary research in order to define the meaning of this crime, each according to their field of specialization, and to dissect it in order to know its motives and put serious solutions to confront it.[1](Hussein, 2016, p21)

First Requirement: The definition of cybercrime

Cybercrime has become a broad topic, and jurists and researchers have differed in giving it a precise definition. The Algerian legislator in 2009 enacted a law for it, which includes the rules for the prevention and combating of crimes related to information and communication technologies, and defined it.

Paragraph 1:Terminologically

In terms of terminology, cybercrime is defined as follows:
"Any crime that can be committed using a computer system or network, or within a computer system. This includes, in principle, all crimes that can be committed in an electronic environment."

One of the definitions that has been expanded is the definition of the American expert "Parker". He tried to give it a broad concept that encompasses all forms of abuse in the field of using information systems. From his point of view, cybercrime is: "Any intentional criminal act, regardless of its connection to information technology, that results in a loss to the victim, or a gain for the perpetrator".[2](turki, 2009, p,p 15, 16)

Cybercrime is a crime related to the manifestations of technological progress. Some call it "crimes of modern technology". Criminologists

have nominated it to develop in the future in view of the modern technologies that appear daily and on a permanent and continuous basis.

Paragraph 2:Legal definition

Legal opinions differed in defining cybercrimes, and we mention some of them as an example:

Rose Nablate defined it as: "An illegal activity aimed at copying, changing, deleting, or accessing information stored inside the computer or that is transferred through it".[3](Michael, 1990, p104)

The German jurist "Zeiber" also defined it, who considered that it falls within the scope of computer crimes: "Any illegal act related to the automatic processing of data or its transfer".[4](Deveze, 2001, p 496)

The jurist Steen Skjolberg defined computer crimes by saying: "Any illegal act for which knowledge of information technology is essential for its perpetrator, investigation, and judicial prosecution".[5](Mahmoud Ahmed, 2005, p16)

The French jurist Massi defined it by saying: "Legal attacks that can be committed by information technology for the purpose of making a profit".[6](Michael, 1985, p107)

In the same direction, the jurists "Michel and Credo" believe that misuse of the computer includes using the computer as a tool to commit a crime, in addition to cases related to unauthorized access to the victim's computer or data. This crime also extends to include physical attacks on the computer itself, or the equipment connected to it, as well as the illegal use of credit cards, forgery of the physical and moral components of the computer, and even stealing the computer itself or a component of its components.[7](Mohamed Ali, 2004, p45)

The jurist Jamal Saber Naaman believes that the cybercrime is: "The crime that is carried out using a computer through the internet, and its goal is to hack networks or sabotage them or distort or forge or steal and embezzle, or piracy and steal intellectual property rights, and the deviant behavior constitutes a crime with its material and moral pillars, and there is no reference to it in the motive for committing it".[8]

Paragraph 3:The legislative definition:

The Algerian legislator defined cybercrime in Article 2, paragraph (a), of Law No. 09/04 of August 5, 2009, which contains the special rules for the prevention and combating of crimes related to information

and communication technologies, by saying that it is: "Crimes related to information and communication technologies are: crimes against automated data processing systems specified in the Penal Code or any other crime that is committed or facilitated by means of an information system or an electronic communications system".

Based on this article, we can define cybercrime as:"All criminal behaviors in which a computer and its communication networks constitute a means of committing them or a place where they occur, that is, crimes that are committed in the digital environment".

Paragraph (b) of the same article defines information systems as: "Any separate system or group of systems interconnected or interconnected, one or more of which performs automated data processing in accordance with a specific program".

Article 2, paragraph (c) of the same law, defines information data as: "Any process of presenting facts, information, or concepts in a form ready for processing within an information system, including the programs that make the information system perform its function".

Information can be divided into three types:

- Personal information: This is information related to a person's identity.
- Intellectual property information: This is information related to creative works.
- Available information: This is information that is publicly available, such as stock market reports.

Cybercrimes are also known by several other names, including:

- Computer and Internet crimes
- White-collar crimes
- High-tech crimes

Based on these previous definitions, we can conclude the following characteristics of cybercrime:

- It is difficult to identify the perpetrator of the crime, except by using high-tech security measures.
- Cybercrime is the crime of the intelligent, as it does not require the use of force or violence. Intelligence is the key for the cybercriminal to complete his act.
- It is difficult to measure the damage caused by cybercrime, as it is damage that affects entities with moral values, material values, or both.

- Cybercrime is trans-national, as all countries in the world are connected to international telecommunications networks through satellites and the Internet. This has made it a crime that does not recognize the territorial borders of states and has swept the global stage.
- It is easy to fall victim to cybercrime, due to the lack of security controls.
- It is easy to hide and erase the traces of the crime and the evidence that points to the perpetrator.
- It takes refuge in the environment of computers and the Internet. It is a package of data and information in the form of invisible electronic pulses that flow through the information system, making it possible for the cybercriminal to erase the evidence completely.[9](Al- Moumani, 2010, p56)
- It is less physically demanding and violent than traditional crimes.
- It is an unethical behavior in society.
- It is a crime that is not limited to a specific place or time.

Second Requirement: Concept of infiltration

Due to the widespread spread of emerging crimes, especially transnational organized crime and other emerging crimes, this is what made most countries formulate their legislative texts in a way that helps to confront this type of crime, and this by putting in place special procedures that differ from the procedures in ordinary crimes.[10](Al-saeed, kamal, 2021, p45)

Paragraph 1 :Legal definition:

Infiltration is considered to be the work done by the competent security agencies by penetrating and infiltrating the criminal group under investigation, so that it is difficult for the remote observer to identify it, and this requires the member to infiltrate the group to collect the largest possible amount of information, to facilitate the security agencies to know the strengths and weaknesses in it, and then achieve the goal and purpose of the Infiltration.

As a part of the jurisprudence defined it as: "Accessing a place or group in a secret way, and making them believe that the informer is not a stranger to them or their dialogue, and reassuring them that he is one

of them, which makes it easy for him to know their concerns, orientations, and future goals".[11](Fawzi, 2014, 2015, p58)

Others defined it as: "It is a procedure carried out by a judicial police officer or one of his assistants, under the responsibility of the officer, to deceive the persons suspected of committing the crime of crimes considered to be a felony or misdemeanor that he is one of them in order to be able to monitor them in order to reveal the circumstances of this crime and surround its perpetrators".[12](Nabila, 2018, p69)

From here, we conclude that the Infiltration is a technique of investigative techniques that allows a judicial police officer to infiltrate a criminal group, with the aim of following up and monitoring suspected persons, and revealing their criminal activities, and this by concealing his true identity and presenting the informer as an actor or partner to them.[13](Al- saeed, kamal, 2021, p45)

Paragraph 2 :The legislative definition:

By referring to the Code of Criminal Procedure 06/ 22, we find that it has stipulated new methods that are in line with the type of emerging crimes, including infiltration or penetration, and its definition is provided in Article 65 bis 12, which states that infiltration is the penetration and infiltration of a judicial police officer or his assistants into criminal groups, in order to gain their trust, and this is what is stated in the French Code of Criminal Procedure in Article 706-81, paragraph 2.[14](Abdul Karim, 2018, p3)

We conclude that infiltration is an operation carried out by a judicial police officer after planning it in a secret and rigorous manner to monitor the persons who commit emerging crimes, and this by deceiving them in any way that he is a factor with them or a partner to them, and this by hiding their true identity, and he also helps them in criminal acts as if he is one of the criminal group, but on condition of obtaining prior authorization from the competent judicial authorities and under their supervision.

Paragraph 3 : Crimes Related to Infiltration:

The infiltration procedure is carried out in emerging crimes, which have known a wide field in the criminal arena, which are characterized by planning and speed in their implementation. Article 65 bis 5 of the Code of Criminal Procedure has come and limited them to:

- Drug crimes.
- Transnational organized crime.
- Crime affecting automated data processing systems.
- Money laundering crimes.
- Terrorism crimes.
- Crimes related to the legislation on exchange.
- Corruption crimes

SECTION II : The Role of Infiltration in Detecting Cybercrime

Infiltration is a special investigative technique that allows judicial police officers or judicial police officers to penetrate a criminal group, under the responsibility of another judicial police officer responsible for coordinating the infiltration operation, in order to monitor suspects and reveal their criminal activities, by concealing the real identity and presenting the infiltrator as an actor or partner.[15](Abdu Rahman, 2010, p75)

Infiltration is considered a new mechanism in the search and investigation of crimes that are extremely dangerous to the security of the judiciary, as it requires courage, competence, and accuracy in work, must be prepared and organized with precision, targets certain circles, and requires in-depth study because it is direct in the circles of the criminal group, the judicial police officer or the officer in charge enters into contact with the suspects and establishes relations with them in complete secrecy, in order to achieve the goal of the operation, and this measure is resorted to in the investigation phase when necessity requires it.[16](Abdu Rahman, 2010, p74)

First Requirement : The extent of the permissibility of electronic infiltration

Infiltration allows judicial police officers to penetrate into the criminal group, to reveal the perpetrators of crimes and their criminal activities, and the concealment of the police officer's real identity and advancing on the basis that he is an actor or partner. In this case, is it permissible for this person to enter the virtual world and reveal cybercrime? This is what we will address in this section by addressing

the extent of the importance of electronic infiltration, and the position of the Algerian legislator towards it.

Paragraph 1 :The importance of infiltration

The importance of infiltration lies in the fact that it establishes a criminal foundation for information technology that surrounds criminal activity. It is used by judicial police officers around the world, where they recruit their men to enter digital fields through discussion forums, research rooms, and direct contact, using aliases and descriptions in order to sign the perpetrators of crimes and bring them to justice.

The officer impersonates a character to enter the secured and electronically protected areas. The entry is personal and is done by impersonating one of the workers in the secured place. This is done by downloading tapes and discs from the computer, and he appears in the appearance of the person who works in the place and stands in front of the door carrying his own card and waits for someone else with a card. When the door opens, he enters with him, and this leads to the exposure of the criminals.[17](Rabeh, 2017, p76)

Infiltration does not require tremendous efforts or high amounts, as the police officer, after carrying out the legal procedures, can follow up on the crime from his office, in addition to the fact that he is not exposed to any danger, as he uses an alias and cannot be identified no matter how sharp the intelligence of the information criminal is.

The importance of digital infiltration increases for judicial police officers so that they can identify the identities of the criminal group, for easy access to them and follow their movements in the digital environment. Despite the importance of information criminal infiltration, the Algerian legislator has confined these tasks only to the judicial police, and did not allow the recruitment of informants to carry out this task despite the widespread spread of this crime, and the reluctance of victims to report.

Paragraph 2 :The position of the Algerian legislator on infiltration

In view of the seriousness of some crimes, including transnational organized crime, the Algerian legislator has created a set of methods, including intercepting correspondence, recording voices, taking pictures, controlled delivery, and infiltration, in accordance with Law 06/22, which includes the Code of Criminal Procedure.[18] (Asmaa, 2017, p76)

The definition of infiltration is mentioned in Article 65 bis 12 of the Code of Criminal Procedure, in the first paragraph of which: "Infiltration means that police officers or officers under the responsibility of the police officer responsible for coordinating the operation monitor persons suspected of committing a felony or misdemeanor by deceiving them that he is an actor with them or their partner or afraid."

Although the Algerian legislator addressed the process of infiltration, he did not address infiltration in the digital environment. Since the legislator did not restrict infiltration, we believe that there is no objection to the permissibility of infiltration within internet forums and social media sites in all their forms.

We believe that the Algerian legislator should have stipulated infiltration not only in the field of investigating cybercrimes, but in all crimes committed using information and communication technology.

Second Requirement: The legality of infiltration

To give the infiltration process the character of legality, legality requires that the process be surrounded by appropriate guarantees to maintain this right to privacy, based on the rules of law and the rules of ethics.

Paragraph 1 :Conditions for infiltration

Articles 65 bis 11 to 65 bis 18 of the Code of Criminal Procedure came in order to succeed the infiltration process and protect the infiltrant from all dangers. In accordance with the principle of legality, it is necessary for the infiltration process to meet both formal and substantive conditions.

a. Formal conditions:

- Issuance of a permit for infiltration, as stated in Article 65 bis 11 of the Code of Criminal Procedure: ".....The Attorney General or the investigating judge, after notification of the Attorney General, may, under....." The competent authority to issue the permit is the Attorney General or the investigating judge, and this is protection of the rights enshrined in the constitution.

- The permit must be written and motivated, and must include information such as: the nature of the crime, the identity of the police

officer responsible for the operation, and the officer must write the reason for requesting this procedure.[19] (Abdullah, 2011, p281)

- The police officer prepares a report to the Attorney General or investigating judge that includes the necessary elements for the crime scene, so that the judge can determine whether or not to resort to infiltration.[20](Fawzi , 2019, p248)
- The officer must write all information related to the identity of the officer responsible for the operation.
- All elements related to the crime must be mentioned, from the identity of the suspects to the mention of the means used in the crime.[21](
- The time limit for carrying out the operation must be mentioned in the permit granted to the officer, which does not exceed four months (Article 65 bis 15).[22] (Mohamed, 2008, p73)
- The date of the beginning and end of the operation must be mentioned.
- The date of issuance of the permit cannot be the date of the beginning of the operation, but rather extends for a week, for example, from the date of issuance of the permit.
- The police officer must inform the Attorney General of the date of the beginning of the operation.
- The judge may extend the duration of the operation for another four months, if the police officer is unable to stop his activity during the first four months, under conditions that guarantee his security.[23] (Nour-Aldin, 2008, p16)

b. Substantive conditions:

- Due to the seriousness of the infiltration process, there must be motives for resorting to it, as stated in Article 65 bis 11 of the Code of Criminal Procedure: "When the requirements of investigation and its require, after notification of the Attorney General, to authorize under his supervision according to the case to initiate the infiltration process within the specified conditions", meaning that the infiltration that does not seek to benefit from the occurrence of the truth is considered to be controlled infiltration.[24]((Nour- Aldin, 2008, p17)
- Secrecy is very important in the infiltration process, so the officer responsible must surround the operation with complete secrecy (Article 65 bis 16 of the Code of Criminal Procedure).
- Through the text of Article 65 bis 12 of the Code of Criminal Procedure, the person responsible for carrying out this operation is a

police officer, who carries out the process of rigorous and precise organization, and another police officer or police officer is responsible for carrying out this task.[25](Fawzi , 2019, p248)

Paragraph 2 : The extent to which infiltration violates the principle of integrity

Legal rules are no longer the only ones that govern the means of investigating crime. The principle of integrity also contributes to defining the framework within which the search for cybercrime and its evidence is conducted. This principle is based on ethics and the requirements of justice.

The Algerian legislator has not defined the means that can be resorted to in order to investigate crimes. However, most legislations punish trickery as it is considered to be contrary to ethics and the principles of honesty, integrity, and frankness. As for legal scholars, most of them have agreed on the permissibility of resorting to means that contain the meaning of trickery as long as they are looking for the discovery of the crime.[26](Ahmed, 2011, p82)

As for the judicial authorities, such as the prosecutor and the investigating judge, they are not allowed to resort to such means. The resort of the judge to deception is considered an illegal act.

In defining integrity in the field of cybercrime, it is essential to start from the need to respect the will of the suspect and the privacy of his life. The use of trickery by the police officer requires the condition that it does not reach the point of inciting or luring the suspect into committing the crime, and this is under penalty of nullity.

Although infiltration constitutes an procedural means in revealing cybercrimes, it also narrows the space of integrity that should be characterized by the process of searching for evidence and collecting it. This led some to say that "effectiveness does not always agree with integrity".[27](Mutassim Khamees, 2013, p56)

Despite the debate about the legality of this science, the majority of people agree on the permissibility of resorting to trickery in revealing cybercrime, especially since dealing in the digital environment is with a criminal who is characterized by intelligence that can help him to conceal the behavior that constitutes the crime, and there is no room to

reveal this crime except by using trickery. Here comes the role of the judiciary in monitoring the extent to which the necessary guarantees are respected and the principle of integrity is respected.

Conclusion:

The paper concluded that infiltration is a new and effective method for investigating cybercrime. However, it is also a dangerous process that can violate the privacy of suspects. The paper recommends that the Algerian legislator extend the use of infiltration to all crimes committed using information and communication technology, and that it establish safeguards to protect the privacy of suspects. Finally, the paper has reached the following results:

- Infiltration is a new method introduced by the Algerian legislator in Law No. 06/22 of 20 December 2006 amending and supplementing the Code of Criminal Procedure, due to the ineffectiveness of ordinary methods with the proliferation of cybercrime.
- Infiltration is a dangerous process for the judicial police officer or assistant due to his penetration into criminal networks without their knowledge of the identity of the infiltrator.
- All evidence produced by the infiltration process is considered as evidence before the judicial authorities during the investigation.
- The Algerian legislator did not stipulate the obligation to respect professional secrecy in the infiltration process, as he did in regulating electronic surveillance procedures.

Recommendations:

- The Algerian legislator should have stipulated infiltration not only in the field of investigating cybercrimes, but in all crimes committed using information and communication technology.
- The Algerian legislator should allow the recruitment of informants specialized in infiltration operations, not limited to the judicial police only, and subject them to special training for these dangerous operations.
- The legislator should review the date of commencement of the operation, which is from the date of authorization for infiltration and not from the date of its actual implementation, because this leads to the possibility of abuse by the judicial police officer.

- The Algerian legislator should have excluded the forums that take place between lawyers and some defendants within the framework of legal consultation requests on the Internet sites, as well as those that take place between doctors, because this entails violating the right to privacy.
- The Algerian legislator should specify the authority authorized to extract documents, including the fictitious identity of the officer during the operation.

Marginalization :

[1]-Rabeai, Hussein, Mechanisms of Research and Investigation in Cybercrimes, PhD Thesisin Law, Specializing in Criminal Law and Criminel Sciences, University of Hajj Lakhdar,Batna,2016,p 21.
[2]- Moushier, Turki bin Abdul Rahman, Building a Security Model to Combat Cybercrimes and Measuring Its Effectiveness, PhD Thesis, Naif Academy of Security Sciences, Riyadh, 2009, pp.15,16.
[3]- Alexander Michael, Computer Crime, Comuter Word, Vol XXIV, 11, 1990,p 104.
[4]- Lucas, André ,Deveze, Jean,The Law of Computing and the Internet, P,U,Paris, 2001, p 496.
[5]- Abana, Mahmoud Ahmed, Computer Crimes and Their International Dimensionns, Dar AL- Thaqafa for PUblishing and Distribution , Amman, 2005, p 16.
[6]- Massé ,Michel, Infractions, L ordre financier, Rev.sc. crim, No. 1, 1985,p 107.
[7]- Arian, Mohamed Ali, Cybercrimes, Dar Al- Jamiaa, Alexandria, 2004, p 45.
[8]
[9]- Al- Moumani, Abdul Qader Nahla, Cybercrimes, 2nd ed, Dar Al- Thaqafa for Publishing and Distribution, Amman, 2010, p 56.
[10]- Barah, Al-Saeed, Boubaya, Kamal, Innovative Methodz within the Stategy of Detecting Emerging Crimes in Algerian Legislation, Leakage as a Model, Scientific Research Notebooks, volume 9, Issue 1, 2021,p 245
[11]- Lawati, Fawzi, Investigation of Drug Crimes in Light of Special Investigative Methods, Master s Thesis Supplement, University of Algeria 1, 2014, 2015 , p 58.
[12]- Qishhah, Nabila , Leakage as a Mechanism for Investigation and Investigation in Organized Crime, Future Journal for Legal and political Stdies, lssue 03, Centre University of Aflou, June 2018, p 69.
[13]- Barah , Al- Saeed , Boubaya, Kamal , The Previous Referense, p 247.

[14]- Fayzi, Abdul Krim, Sh eikh, Najia, The Procedure of Leakage in Algerian Law : A Means to Combat Emerging Crimes, Ma arifa journal, lssue 13, December 2018, p 03.
[15] - Khalifi, Abdul Rahman, Lectures in Criminal Procedure Law, Dar Al- Huda, Algeria, 2010, p75.
[16] - The Same Reference, p 74.
[17]- Howa, Rabah, Research and lnvestigation in Cybercrime, Master s Thesis Supplement, Specilalizing in Criminal Sciences, University of Abbas Laghrour, Khenchela, 2014, p 143.
[18]- Anter, Asma, Combating Emerging Crimes in Algerian Legislation : Leakage as a Model, Journal of Algerain Public Law and Comparative Law, lssue 6, 2017, p 76.
[19]- Ouhaiya, Abdullah, Explanation of Criminal Procedure Law, 2 nd ed, 2011, p 281.
[20]- Amara, Fawzi, lnterception of Correspondence, Recording of Sounds, Taking Pictures, and Leakage as a Judicial lnvestigation Procedure in Criminal Matters, Journal of Human Sciences, University of Mentouri, Constantine, lssue 33, 2019, p 284.
[21]- Ouhai, Abdullah , the Previous Reference, p 281.
[22]- Hazit, Mohamed, Notes in Algerian Criminal Procedure Law , 3rd ed, Dar Houma, Algeria, 2008, p 73.
[23]- Lojani, Nour El-Din, Methods of Vertical Research on the Relationship of the Judicial Police with the Public Prosecution and Respect for Human Rights, Article Published in the Police School, Taybi Al- Arabi, Algeria, 2008, p 16.
[24]- The Same Reference, p17.
[25]- Amara, Fawzi , the Previous Reference, p 248.
[26]- Musha sha a Mutassim Khamees, Proving Crime with Scientific Evidence, Journal of Sharia and law, lsse 56, 2013, p 56.
[27]- Ghazi Ahmed, Concise Guide to Organizing the Tasks of Judicial Police, 5 th edition, Dar Huma, Algeria, 2011, p 82.

List Of References

- Abana, Mahmoud Ahmed,(2005), Computer Crimes and Their International Dimensionns, Dar AL- Thaqafa for PUblishing and Distribution , Amman.
- Al- Moumani, Abdul Qader Nahla, (2010), Cybercrimes, 2nd ed, Dar Al- Thaqafa for Publishing and Distribution, Amman.
- Alexander Michael,(1990), Computer Crime, Comuter Word, Vol XXIV, 11.

- Amara, Fawzi,(2019), lnterception of Correspondence, Recording of Sounds, Taking Pictures, and Leakage as a Judicial Investigation Procedure in Criminal Matters, Journal of Human Sciences, University of Mentouri, Constantine, lssue 33.
- Anter, Asma,(2017), Combating Emerging Crimes in Algerian Legislation : Leakage as a Model, Journal of Algerain Public Law and Comparative Law, lssue 6.
- Arian, Mohamed Ali,(2004) Cybercrimes, Dar Al- Jamiaa, Alexandria.
- Barah, Al-Saeed, Boubaya, Kamal,(2021), Innovative Methodz within the Stategy of Detecting Emerging Crimes in Algerian Legislation, Leakage as a Model, Scientific Research Notebooks, volume 9, Issue 1.
- Fayzi, Abdul Krim, Sh eikh, Najia,(December 2018), The Procedure of Leakage in Algerian Law : A Means to Combat Emerging Crimes, Ma arifa journal, lssue 13.
- Hazit, Mohamed,(2008), Notes in Algerian Criminal Procedure Law , 3rd ed, Dar Houma, Algeria.
- Howa, Rabah,(2014) Research and lnvestigation in Cybercrime, Master s Thesis Supplement, Specilalizing in Criminal Sciences, University of Abbas Laghrour, Khenchela.
- Ghazi Ahmed,(2011), Concise Guide to Organizing the Tasks of Judicial Police, 5 th edition, Dar Huma, Algeria.
- Khalifi, Abdul Rahman,(2010), Lectures in Criminal Procedure Law, Dar Al- Huda, Algeria.
- Lawati, Fawzi,(2014, 2015), Investigation of Drug Crimes in Light of Special Investigative Methods, Master s Thesis Supplement, University of Algeria 1.
- Lucas, André ,Deveze, Jean,(2001),The Law of Computing and the Internet, P,U, Paris.
- Lojani, Nour El-Din,(2008), Methods of Vertical Research on the Relationship of the Judicial Police with the Public Prosecution and Respect for Human Rights, Article Published in the Police School, Taybi Al- Arabi, Algeria.
- Massé ,Michel,(1985), Infractions, L ordre financier, Rev.sc. crim, No. 1.

- Musha sha a Mutassim Khamees,(2033), Proving Crime with Scientific Evidence, Journal of Sharia and law, lsse 56.
- Moushier, Turki bin Abdul Rahman, (2009), Building a Security Model to Combat Cybercrimes and Measuring Its Effectiveness, PhD Thesis, Naif Academy of Security Sciences, Riyadh.
- Ouhaiya, Abdullah,(2011), Explanation of Criminal Procedure Law, 2 nd ed.
- Qishhah, Nabila ,(June 2018), Leakage as a Mechanism for Investigation and Investigation in Organized Crime, Future Journal for Legal and political Stdies, lssue 03, Centre University of Aflou .
- Rabeai, Hussein,(2016), Mechanisms of Research and Investigation in Cybercrimes, PhD Thesisin Law, Specializing in Criminal Law and Criminel Sciences, University of Hajj Lakhdar,Batna.