INSPECTION PRIVACY IN THE DIGITAL ENVIRONMENT

Dr. Mehdaoui Mohammed Salah[1], Khelifi Fatiha[2]

[1] University Belhadj Bouchaib of AinTemouchent, Faculty of Law, The laboratory examines the operation, legislation, and jurisdiction of markets in the Maghreb countrie, Algeria, mohammed.mehdaoui@univ-temouchent.edu.dz
[2] Phd student, University Belhadj Bouchaib of AinTemouchent, Faculty of Law, The laboratory examines the operation, legislation, and jurisdiction of markets in the Maghreb countries, Algeria, Fatiha.khelifi@univ-temouchent.edu.dz

ABSTRACT

This research studies crime inspection in the digital environment. Ithas characteristics that distinguish it from inspection in its traditional sense. It is about the way the crime is committed, which is the computer. Inspection of the digital environment also requires objective and formal controls in order to be properly performed.

Keywords: Inspection, Crime, Digital environment, Privacy, Controls.

INTRODUCTION

The technological development that the world has witnessed has led to the emergence of so-called cybercrimes, which are new crimes that are committed in a digital, virtual environment by means of a computer and various communication networks. They differ from traditional crimes in terms of how they are committed and the crime scene.

Therefore, one of the major difficulties facing investigators in information crimes is the difficulty of searching for evidence in order to prove it and attribute it to its perpetrators, and this is due to the specificity of the evidence in these crimes so that it can be disposed of, destroyed, and even manipulated and hidden in devices located outside the territory of the country in which the crime was committed. This is to mislead the investigators and prevent them from uncovering the truth.

And since crime inspection in the digital environment requires accurate investigation procedures, as it focuses on the computer and the information networks connected to it, this requires high professionalism and great skill in order to access documents related to the crime.

The importance of the topic highlights the urgent need to study its characteristics and controls, as inspection in the digital world is a complex and intertwined process that is completely different from inspection in traditional crime. Which necessitates combating this crime by identifying its investigation techniques and inspection controls.

And based on the importance of the topic, we can pose the problem as follows: Can inspection of crime in the digital environment be considered a special kind of inspection? In other words, how private is the search in the digital environment?

In order to address this issue, we relied on the descriptive approach in terms of describing and defining the term inspection and its characteristics, in addition to the analytical approach through analysing the extent to which computers and information networks can be subjected to inspection.

In order to answer the problem at hand, we decided to divide the subject into two sections. In the first topic, we dealt with the nature of inspection in the digital environment, and in the second topic, we dealt with the inspection controls in the digital environment.

The first topic is the nature of inspection in the digital environment.

Information crimes are characterized by a special nature as they are committed in a virtual world. Therefore, the process of searching for evidence is difficult and complex and requires an inspection that suits the virtual environment. The digital environment (second requirement) within it

The first requirement is the concept of inspection in the digital environment.

In order to be able to define the concept of inspection in light of the digital environment, we must address the definition of inspection and its importance (Part One), then define its legal nature (Part Two) and its characteristics (Part Three).

The first section: the definition of inspection and its importance

We discuss the definition of inspection in the digital environment first, and then its importance second.

First: defining inspection in the digital environment.

Inspection, in its traditional sense, is a procedure aimed at preserving material things related to the crime and useful in revealing the truth. Jurists have differed in defining inspection. Some define it as a procedure of investigation aimed at searching for material evidence about a felony or misdemeanour and proving its commission or attributing it to the accused according to specific legal procedures. While others defined it as an investigative procedure, it is not an administrative act of administrative control but rather an investigation and judicial investigation to collect evidence of a specific crime after the accusation against a specific person .

Inspection in the digital environment was defined by the European Council as a procedure that allows the collection of evidence stored or recorded electronically[4] and is also defined as an investigative procedure to search for evidence of a digital crime on a computer or any smart device.

The inspection and confiscation of computers and information storage systems is an important means of detecting electronic crimes.

By presenting these definitions, we conclude that the inspection in the digital environment focuses on the storage systems of the computer in order to access the data that it saves, as it is an inspection of the virtual digital space.

Second: the importance of inspection in the digital environment.

Inspection in the digital environment is of great importance, which is manifested in determining the degree of danger of the offenders and their criminal style in the event that discs containing decoding programs, virus programs, books on famous computer crimes, or qualifications indicating that the accused is a specialist and professional in the field of computers and networks are found. As this would reveal the criminal's style whether by the quality of the stolen goods or by accessing the information network or websites, and the perpetration of the incident and the degree of its criminal severity, and this is useful to the criminal investigator in determining the ways to deal with the accused, whether at the time of arrest or at the time of indictment, and its importance is also evident in proving the occurrence of the crime, its elements, its conditions, and its real time and place incident, as well as determining the real motive behind the commission of the crime, and therefore it can be said that this importance is achieved by the inspection, whether in conventional crimes or in the digital environment , the desired goal through the inspection process is to uncover evidence of the crime and find the perpetrators.

The second section the legal nature of inspection in the digital environment.

The legal nature of the search in the digital environment is that it is an investigative procedure that is ordered only by one of its authorities when a crime, a felony, or a misdemeanour is considered to have occurred. It aims to collect evidence of the crime committed and its perpetrators, and this means the investigation is not evidence but rather a means of obtaining evidence. So investigation is a procedure that allows using certain actions to find the evidence sought. It also has a legal effect in the sense that if the search is invalid, all the procedures and actions resulting from it are tainted with invalidity. So the search is an act of primary investigation that takes place after a public lawsuit is initiated with the intent of revealing the truth.

The third section is Characteristics of Inspection in the Digital Environment.

Among the characteristics that can be drawn from the previous definitions, which characterize inspection in the digital environment, are the following:

Inspection is one of the investigation procedures, as the legislator stipulated in Law 04-09 that for the

requirements of inquiries and investigations, the specialist judicial authorities as well as judicial police officers may enter, for the purpose of inspection, even remotely, an information system or part of it, as well as the information data stored in it, as well as an information storage system.

The inspection is carried out by a team consisting of:

- The main investigator, who has experience in criminal investigation

- Computer and Internet experts who know how to deal with such crimes

- Experts in controlling and editing digital evidence who are familiar with computer searches

- Computer experts who deal with software systems

- Experts in photography, fingerprints, and diagrams.

Inspection in the digital space is characterized by the fact that it is a complex and intertwined process that requires those in charge to have extensive knowledge and high efficiency in searching for information and in processing, analysing, and deciphering data. And this becomes harder as computer hard disk space gets larger, which results in large files that need to be decoded and analysed.

Violating the right of the accused to keep their secrets and the sanctity of their home, as the search is an assault on human freedom and rights and a violation of his sanctity , and it is a serious infringement on private life as it includes the development of technical arrangements to monitor electronic communications, and it includes recording and simultaneous and immediate collection of these communications as well as conducting searches and seizures within information systems, perhaps the obvious example is the traces left by the internet surfer through which a huge amount about their private life is collected.

Inspection in information crime is carried out by specific agencies such as the National Institute of Forensic Evidence and Criminology under the General Command of the National Gendarmerie, the Information and Electronic Department that specializes in information crimes, which was created by Presidential Decree No. 04-183 of June 26, 2004, as well as the Center for Preventing and Combating Cybercrimes.

The second requirement is: The location of inspection in the digital environment

The principle is that the location is the place where the inspection process takes place, and with regard to traditional crimes that leave physical traces, its place does not raise any problems because it takes place in tangible physical places. As for electronic crimes, the place of inspection in it is a digital space, and since this type of crime is committed by computers, it is considered a place for inspection in information crime, which consists of three components. Therefore, when we perform the process of inspecting the computer, we are in front of three scenarios, which makes us wonder about the extent of the susceptibility of the computer components to inspection. Second) Inspection of computer-related information networks (third branch)

The first section: Inspection of the physical components of the computer.

The jurists unanimously agree that the physical components of a computer are suitable to be searched, in the sense that the ruling on those components depends on the nature of the place in which they are located, as the latter has a special importance in the inspection process. So if the computer components existed in a specific location, the suspect's home, for example, the same rule applies, as these components may not be searched except in cases where it is permissible to search the dwelling or the private place, and the same applies to the presence of computer components in a public place, so the rules and guarantees of searching those places and persons are applied to them if they are in their possession. Inspection of the physical components of the computer, such as hard disks or electronic processors, cables, keyboards, and printers, in search of evidence related to digital crime does not constitute any obstacle.

Thus, it can be said that the inspection of the physical components of the computer is subject to the same inspection process as in traditional crimes, as it focuses on tangible physical evidence, but the inspection process needs to be conducted by trained professionals, and this is in order to preserve these components and not sabotage or destroy them.

The second section: Inspection of the intangible components of the computer

If the jurisprudence was unanimous on the possibility of inspecting the physical components of the computer, then the matter differs regarding the possibility of inspecting the intangible components in order to control the evidence, and a jurisprudential controversy has arisen regarding this issue.

The dispute that occurred in the issue of the search being a means of searching and seizing traces related to the crime and presenting them to the court as evidence of conviction, so the question arises about the possibility of considering the search for evidence of electronic crime in computer systems and programs as a kind of inspection, given that electronic data or programs in themselves lack an appearance tangible material in the external environment and jurisprudence senses the difficulty of the issue in view of the absence of the material nature of information and data, which makes it inconsistent with the goal that the search aspires to, which is the search for physical evidence, and this prompted the French legislator to amend the provisions of the search by Law No. 2004-545 of June 21, 200', where the phrase "informational data" was added in the text of Article 94 of the French Code of Criminal Procedure.

The European Convention on Information Crime signed in Budapest in 2001 stipulates that each party must adopt legislative procedures or any other procedures it deems necessary in order to authorize its competent authorities with the power of inspection or access in a similar way to an information system or part of it, as well as to the information data stored in it and on its territory, and to an information storage support that allows the storage of information data. This agreement provides for inspection in the digital environment.

Among the Arab legislations that allow inspection in automatic data processing systems is the Jordanian law in the text of Article 31/1 of the Code of Criminal Procedures, where it states, taking into account the terms and conditions established in the relevant legislations, that judicial police employees may enter any place suspected of being used to commit any of the crimes stipulated in this law, and they may also inspect devices, tools, progcrimessystems, and means suspected of being used. As for the Algerian legislator, according to Article 5 of Law 09-04, to inspect an information system or part of it, as well as an information storage system, he has followed the example of the French and Jordanian legislators.

The third section: Inspection of computer-related information networks

It is called a remote search, because the nature of digital technology has complicated the challenge in front of the inspection and control work, due to the extension of electronic evidence through computer networks in places far from the physical location of the inspection, although it is possible to access it through the computer after obtaining a search permit, and the actual location of the data may be within another jurisdiction or even in another country, which complicates the issue, given that the information network extends almost all over the world, and therefore the computer on which the information crime can be committed is subject to the procedural law of that region, and here we distinguish between two hypotheses :

First, the accused's computer is connected to another computer, or the end of its terminals is located in another place within the country.

The issue that arises in this case is when the accused's device is connected to another device owned by another person in another place, but in the same country. In this case, the authority conducting the search may have exceeded its spatial jurisdiction when searching the device connected to the device of the accused. In this case, the problem of infringement on the privacy and secrets of other people who have nothing to do with the crime also arises.

Among the legislations that dealt with this problem, we find German jurisprudence, as it recognizes the possibility of extending the search to the data records that are located in another place based on what was stipulated in Section 103 of the German Code of Criminal Procedure, when the actual storage location is outside the place where the inspection takes place, as Article 88 of the Belgian Code of Criminal Procedure stipulates that "If the investigating judge orders a search in an information system or part of it, this search can extend to another information system located in a place other than the place of the original search, if it is necessary to uncover The truth about the crime in question, and if there are risks related to the loss of some evidence due to the ease of erasing, destroying or transferring the data in question.

As for the Algerian legislator, we find that the possibility of extending the inspection has been acknowledged in Article 5/2, which reads: "If there are reasons to believe that the data in question are stored in another information system and that these data can be accessed from the first system, the inspection may be quickly extended to this one." The system or part thereof after notifying the specialist judicial authority in advance.

Second, the accused's computer is connected to another computer located elsewhere outside the country, and the problem that arises in this case is more complex than in the previous case, as the perpetrators of information crimes store information, which is considered evidence of their commission of these crimes and their conviction, on another device located in a foreign country. Their goal behind this is to mislead the investigation process so that they are not caught.

And the extension of the inspection to the computer systems located in a foreign country is important as it

makes it possible to obtain evidence remotely and, in a few seconds, but jurisprudence reserves the right to do so because it is considered a violation of the sovereignty of a foreign country, and if the necessity of the investigation requires doing so, many guarantees must be taken into account. in advance through agreements and treaties in this field, and this confirms the importance of international cooperation in combating cybercrime

In this context, the European Council issued recommendations that allow the extension of the inspection outside the territory of a country, as stipulated in Recommendation No. 13 of 1995 related to the legal problems of the Criminal Procedure Law related to information technology, in which it was stated that "the investigating authority, when carrying out the inspection of information according to certain controls, may extend the scope of searching a specific computer that falls within its jurisdiction to other devices as long as it is connected to one network, and seizing the data in it as long as immediate intervention is necessary to do so."

Article 32 of the European Convention on Information Crimes also stipulates the possibility of accessing, for the purpose of inspection and seizure, devices or networks belonging to another country without its permission in two cases: the first if the inspection is related to information that is available to the public, and the second if the owner of this data consents to this inspection.]

As for the Algerian legislature, it has permitted the possibility of inspecting information networks connected to computers even if they are located outside the country, through Article 5/3 of Law 09-04, which states, "If it is found in advance that the data in question and which can be accessed from the first system stored in an information system located outside the national territory, access to it shall be with the assistance of the specialist foreign authorities in accordance with the relevant international agreements.

The second topic is inspection controls in the digital environment.

The inspection process in the digital environment requires certain controls in order to combine the protection of society, which requires punishment for the criminal, with the protection of people and respect for their privacy. Through this topic, we are exposed to these controls, which are divided into objective controls (the first requirement) and formal controls (the second requirement).

The first requirement is objective controls for inspection in the digital environment.

In order for the inspection process to be valid, objective conditions must be met, and they precede the inspection process, so it is called objectivity, which can be limited to four conditions that we recognize through this requirement, namely, the existence of a reason for the inspection (first branch), the competent authority for inspection (second branch), permission to search (branch three), and the place of inspection (branch four).

The first subsection is the existence of a reason for the search.

The reason for inspection in crimes in general is to seek evidence in an ongoing investigation in order to reach the truth, and it is represented in the occurrence of a crime, a felony, or a misdemeanour, accusing a specific person or persons of committing or participating in a crime, and the availability of evidence and strong indications that there are useful in revealing the truth about the suspect or the accused, or in their residence, or with another person's residence, which applies to cybercrime.

There is no way to conduct an inspection if the investigator does not have sufficient reasons to believe that there are tools in the place or with the person to be searched that were used in the commission of the crime or things obtained from it. The occurrence of a crime and the presence of the accused are not reasons enough to prove a crime, and for the Algerian legislator, it is permissible to search information systems and storage systems for the requirements of investigations or judicial investigations when it is difficult to reach the result of an ongoing investigation. It is not a condition for inspection in information systems that evidence is available for access for the purpose of inspection, but rather that it is possible to obtain evidence.

Section Two: The specialist authority for inspection

In principle, the inspection of computer systems is carried out by the original investigative authority, which is the Public Prosecution, as it is one of the investigation procedures in accordance with the procedural rules stipulated in this regard. However, the legislation did not follow a uniform pattern in defining this authority. As we find that the Egyptian legislation granted it to the Public Prosecution, where the Criminal Procedure Code was issued under Law No. 150 of 1950, and it reverted once again to the system of combining the powers of investigation and indictment in the hands of the Public Prosecution, with the exception of certain crimes, which were considered to be reserved for the investigating judge, unlike Algeria and France, where the system of separation between the powers of accusation and investigation was used, as the latter was assigned to the ivestigating judge while the former was entrusted to the Public Prosecution.

Section Three: Search Warrant

Most jurists believe that the search warrant must specify the place to be searched and the person or things to be searched and seized. The aim of this specification in the search warrant is to avoid exploratory searches so that the inspector is not left with any discretionary power in that, but there is difficulty in respecting this condition during The practical practice of searching computers is due to the special nature of the latter, as the computer contains a large number of files, and the names of these files do not necessarily indicate what they contain. It requires judicial authorization independent of the other, especially as the accused may deliberately use pseudonyms for files. It contains illegal materials. Concerning the Algerian legislation, it did not address this condition through Law 04-09. However, in the event of an extension of the inspection, it is necessary to inform the specialist judicial authority in advance of this, and this is in Article 5/2.

Section Four: The Place of Inspection.

It is also required for the validity of the search to focus on a place, and the location of the search means the place where the person keeps the material secrets, because the search does not focus on the intangible secrets that the person keeps within himself, and therefore they cannot be accessed by inspection but rather by other means such as interrogation or confession, and the inspection location in the digital environment could be a person or a home.

First: What is meant by the person as a place for inspecting computer systems? The person as a place for inspecting computer systems may be one of the exploiters or users of the computer or one of the experts in programs, whether system programs or application programs, and may be one of the analysts or one of the maintenance and communications engineers, the security of information systems managers, or any other persons who possess devices, information equipment, or portable computers. In all cases, the person means as a searchable object everything related to the person's physical entity and what is related to it.

Second: what is meant by houses and the like as a place for inspecting computer systems, and it means all the places of residence or the place and the accessories designated for their benefits and which the person uses, whether permanently or temporarily, and whether they are physical or logical or private communication networks, and the inspection process here is subject to the same conditions and rules of the inspection procedures of houses, and the place of inspection is required to be specific in order to preserve the rights and freedoms of individuals, as it is not possible to search an entire neighborhood, and it must also be from what may be searched, as there are people and places that are excluded from inspection, such as the homes of the diplomatic officials.

The second requirement is formal controls for inspection in the digital environment.

In addition to the objective controls, the inspection must include, in order for it to be valid, formal controls, which are represented in determining the date of the inspection (first branch), the presence of the persons appointed by law for the inspection process (second branch), and issuing a record of the inspection process (third branch).

Section one: Determining the date of the inspection

Among the formal guarantees imposed by the traditional texts in most criminal procedure laws, there are guarantees related to the dates of the inspection, so that certain times are set and it is forbidden to do it outside these times. For example, inspection at night is only allowed in some cases excepted by the legislator specified by legal rules, such as pursuing a fugitive or a person caught in flagrante delicto , and the Algerian legislator specified the period of inspection. Within the Code of Criminal Procedures, it stipulates that it is not permissible to start searching homes before five o'clock in the morning or after eight o'clock in the evening, unless the owner of the house requests that, or appeals are made from within, or in the exceptional cases stipulated in the law.

The second subsection: the presence of certain persons appointed by law for the inspection process.

This condition is considered one of the most important formal conditions, and its purpose is to reassure the subject of this inspection that the proceedings are done in accordance with the law and to prevent the arbitrariness of the authority that conducts them.

And with regard to the Algerian legislator, it was stipulated that, in order to carry out the inspection process in the data stored in the information system, the application of the attendance rule in application of the provisions of Article 5 of Law 09-04, which refers to the general provisions stipulated in the Code of Criminal Procedures, and therefore it requires the presence of the owner of the residence suspected of committing the crime, or the

owner of a residence of a third party possessing papers or things related to the crime for the inspection process or their representative, or the presence of two witnesses if they are unable to attend according to what is stipulated in Article 45 of the Code of Criminal Procedures.

Third Section: Preparing a Record of the Inspection Process

The accepted rule is that all investigation work should be written, and writing includes all investigation procedures, whether it is examining, hearing witnesses, or inspection procedures. With the intent of protecting individual freedoms and preventing arbitrariness, the Algerian legislator obligated the judicial police officers assigned to the investigation to write records confirming the procedures they carried out, indicating the procedures, and the record in general has a set of data that must be available in addition to the persons qualified to prepare it Regarding the form of the record, the Algerian legislator didn't impose a special form in the inspection report, and therefore it does not require anything other than what is required by the rules in the report in general for its validity. That is, it must include all data related to the inspection process and indicate the capacity of the person in charge. The purpose of preparing the report is to determine the extent of compliance with the inspection procedures, which, when not adhered to, would render the inspection process invalid.

CONCLUSION:

Through this study, we have touched on the privacy of the inspection in the crime that is committed in the virtual digital space, as an inspection of a special kind that includes the development of technical arrangements that affect private life and is assigned to specific devices, just as the place of inspection in the digital environment is focused on the computer. It is the tool by which electronic crime is carried out, and in order for the inspection to be carried out in a correct manner, it must have a set of objectives and formal controls.

Based on the results obtained,we can conclude the following recommendations:

The necessity of preparing and training security staff whose task is to investigate crime in the digital environment so that the search for it is not random and by sheer chance.

Since the inspection may extend to other countries, international agreements must be arranged in order to impose cooperation between countries in the inspection process and specify the procedures for carrying it out.

-Requiring investigators to follow technical rules in order to preserve and not destroy data, and in the event that evidence is found within this data, only data related to thecrime will be copied in order to preserve the privacy of individuals.

REFERENCES

1. Rabhi Aziza, Informational Secrets and Their Criminal Protection, a thesis submitted for a PhD in Private Law, Faculty of Law and Political Science, Abu Bakr Belkaid University of Tlemcen, 2017-2018, p. 279.

2. Driss Qarfi, Inspection of stored information data as a procedural mechanism between the Budapest Agreement and Algerian legislation, Journal of Rights and Freedoms, University of Mohamed Kheidar Biskra, Issue 2, issued in 2014, p. 100.

3. Reda Hamisi, Inspection of Information Systems in Algerian Law, Journal of Legal and Political Sciences, Al-Wadi University, Issue 5, issued in June 2012, p. 160.

4. Dear Rabhi, previous reference, p. 279

5. Mustafa Abdel-Baqi, Investigating and Proving Cybercrime in Palestine, a Comparative Study, Journal of Sharia and Law Studies, Bir Zeit University, Ramallah, Issue 4, issued in 2018, p. 289.

6. Abdullah bin Abdulaziz bin Abdullah Al-Khathami, Inspection of Information Crimes in the Saudi System, An Applied Study, a thesis submitted to complete the requirements for obtaining a master's degree in criminal justice, College of Graduate Studies, Naif Arab University for Security Sciences, Riyadh, 2011, p. 41.

7. Manea Salma, Inspection as a Procedure for Investigating Information Crimes, Journal of Human Sciences, University of Mohamed Kheidar Biskra, Issue 22, issued in June 2011, p. 230

8. Muhammad Ali Skaiker, Information Crime and How to Address It, 1st Edition, Al-Jumhuriya Press House, Cairo, 2010, p. 103.

9. Ahmed Raad Muhammad Al-Jilawi, Audio Recording and its Inference in Criminal Evidence, 1st Edition, The Arab Center for Publishing and Distribution, Cairo, 2018, p. 87.

10. Abdullah bin Abdul Aziz bin Abdullah Al-Khathami, previous reference, pg. 42.

11. Qarfi Idris, previous reference, p. 102.

12. Fayez Muhammad Rajeh Ghallab, previous reference, p. 328.

13. Law No. 04-09 of August 5, 2009, containing special rules for the prevention and combating of crimes related to information and communication technologies, C, R No. 47, of August 1, 2009.

14. Qarfi Idris, previous reference, p. 101.

15. Khaled Marzouk, Siraj Al-Otaibi, Procedural Aspects of Attempting Informatics Crimes, A Comparative Study, 1st Edition, Library of Law and Economics, Riyadh, 2014, p. 90.

16. Reda Hamisi, previous reference, p. 163.

17. Qarfi Idris, previous reference, p. 109.

18. Ben Farida Mohamed, Criminal Proof of Information Crimes with Digital Evidence, a thesis for obtaining a PhD in Criminal Law and Criminal Sciences, Faculty of Law, University of Algiers 1, 2015, p. 130.

19. Fayez Mohamed Rajeh Ghallab, Information Crimes in Algerian and Yemeni Law, a thesis for obtaining a PhD in Criminal Law and Criminal Sciences, Faculty of Law, University of Algiers 1, 2010-2011, p. 308.

20. Lamia Majdoub, Inspection Procedure for Electronic Forgery, Journal of Communication in Economics, Administration and Law, University of Badji Mokhtar Annaba, Issue 3, issued in September 2019, p. 111.

21. Brahimi Jamal, Criminal Investigation of Electronic Crimes, a doctoral dissertation, Faculty of Law and Political Science, Mouloud Mamari Tizi Ouzou University, 2018, p. 18.

22. Lamia Majdoub, previous reference, p. 112.

23. Article 19 of the Budapest Convention (European Convention on Information Crimes) dated 08/11/2001.

24. Bin Faridah Muhammad, previous reference, p. 134.

25. Linda Ben Talib, Inspection in Information Crime, Journal of Legal and Political Sciences, Hamma Lakhdar University in the Valley, Issue 16, issued in June 2017, p. 490.

26. Osama bin Ghanem Al-Obeidi, Searching for Evidence in Information Crimes, Arab Journal for Security Studies and Training, Institute of Public Administration, Riyadh, Issue 58, D, T, P, pp. 91-92.

27. Bin Faridah Muhammad, previous reference, p. 141.

28. Linda Bin Talib, previous reference, p. 492.

29. Ilham Ben Khalifa, Inspection as a Traditional Investigation Procedure for Collecting Evidence of Crimes Related to Information and Communication Technologies, International Journal of Legal and Political Research, Hamma Lakhdar Al-Wadi University, Issue 1, d, t, p. 33.

30. Al-Maamari Adel Abdullah Khamis, Inspection in Information Crimes, Police Thought Journal, Emirates Police Research Center, Issue 86, issued in July 2013, p. 264.