Methods of proving cybercrime

Dr. Mehdaoui Mohammed Salah[1]

[1]University Belhadj Bouchaib of Ain Temouchent, Faculty of Law, The laboratory examines the operation, legislation, and jurisdiction of markets in the Maghreb countries **(**Algeria**)**.

Email Author:mohammed.mehdaoui@univ-temouchent.edu.dz

Abstract:

Digital crime is one of the topics that faced so many difficulties. The reason for this is the artificial environment where these crimes are committed. The difficulty mainly lies in the absence of any physical proof that can be used to condemn criminals. Add to this the inefficacity of the traditional mechanisms, which demands more developed tools that match the advanced technological level that characterizes the virtual environment. Many legislations worked towards achieving this and the Algerian legislator is one of them.

key words: Digital crime, Proof, virtual environment, traditional mechanisms, modern mechanisms.

Tob Regul Sci. ™ 2023;9(1): 4353-4378

DOI: doi.org/10.18001/TRS.9.1.304

Introduction:

In recent decades, the world has witnessed a new era where information and digital knowledge are the main components of its infrastructure. Resulting in the appearance of the so-called information technology, which has radically changed the lives of individuals and communities in all domains the political, economic, and social ones. Consequently, the world has moved from the physical to the digital virtual sphere.

Nowadays the process of communication between people and monitoring what is happening in different parts of the world is much easier and this takes only a few seconds making human life easier. Where information technology and communication networks became indispensable tools in daily life. Moreover, due to the increased use and demand of the latter, this pushes a minority to use it in an illegal act. When it comes the motives for committing those crimes differ but the result remains the same which is digital crimes. This type of crime takes place in virtual environments far away from the real world. Add to this type of crime is extremely different from traditional crimes where is difficult to reach physical proof left by its perpetrators. This made it unique when it comes to privacy, where so many questions have been asked on how well to combat this crime mainly when it comes to the process of proving it.

Here stems the importance of the topic of proving the digital crime. Taken into account the failure of practical reality as well other previous laws when it comes to proving this. The main reasons for this failure could be summarized in the following: first of all the mechanisms set for this purpose are more appropriate and suitable for conventional crimes. Moreover, the conditions where those mechanisms are first set differ from that of information technology. What makes this topic more vital is the increasing number of crimes. This requires urgent solutions from legislation including the Algerian legislation to issue legal laws that match the specific nature to come up with tools that can help in the process of proving this type of crime. Especially since many criminals are free and are not receiving the right penalty because investigations are not backed up with evidence.

For this study, the descriptive and the analytical approach were used. The first one is used to describe and highlight the main characteristics of this type of crime. Whereas the analytical approach is more appropriate especially when it comes to analyzing and discussing the different mechanisms that are followed in the process of proving. Following all that has been mentioned above. The following questions have been raised: what are the procedural mechanisms used to prove digital crime? In other words, do we need specific mechanisms to prove digital crime due to its specific nature?

This study is divided into two sections: the first one is about the specific aspects of digital crime. Whereas the second one is about proving it.

SECTION I : SPECIFIC ASPECTS OF DIGITAL CRIME

Digital crime is looked at as a unique type of crime this mainly comes from its relation with modern technology tools in addition to information technology. To understand this first the term digital crime will be defined, followed by its motives.

First Requirement: The concept of Digital Crime.

Many researchers have searched the topic of digital crime without being able to reach one definition for this concept. Due to its ongoing relationship with development and its infinite relation with information technology. First, the definitions of this concept will be provided. Followed by its main characteristics.

Paragraph1: Definition of Digital Crime

When discussing the topic of digital crime so many concepts arise like cybercrime, information crime, and computer and social networks crime. They may seem different but they are all classified under digital crime. Because this crime is committed in a virtual environment, the concept of digital crime is the one that will be used in this study. Due to the different names that refer to this crime the study will start by defining this concept from a legal point of view then it will be followed by a jurisprudence definition.

1- Legal definition for the digital crime.

Law 04-15 (Law 04-15, 2004) marked the issuance of the legislative laws that have relation to digital crime. Where this was ignored by the Algerian legislator but the enactment of the above-mentioned law has filled the gap that already existed about this crime. The provisions of section seven repeatedly criminalize the violation of the automated data processing system. What could be noticed while reading the texts of this law is that no fixed definition was put by the legislator. Where only acts that are found in this type of crime were criminalized. This can be foundin article 394 bis:

Log in to the automated data processing system.

- Deleting or changing the data of the system.

-Damaging the operating system through illegal access.

Add to this other acts are also found in article 394 bis2 :

-Designing,researching, compiling, disseminating, or trafficking in stored, processed, or transmitted data through an information system by which the offenses outlined in this section can be committed.

-Possession, disclosure, publication, or usage of the collected data for any purpose, which are set in this section.

The Algerian legislator issued another law 09-04, (Law N 09-04, 2009) which came as a response due to the many criticisms that the previous law received. According to article 2 of this law, digital crime is defined as the offenses committed against automated processing systems of data specified in the Penal Code or any other offense committed or facilitated through an information system or electronic communication system.

What can be deduced from the new law is that the Algerian legislator is more flexible in terms of the newly issued law, in that it did not limit the acts that could be considered digital offenses which were found in the first one. Where the above-mentioned law did focus on all the acts that are difficult to control and limit, as a result of the rapid development of the perpetration means used in this crime. Hence, this put the legislator in a more developed position in concordance with digital crime.

The French legislator also issued several laws to combat digital crime. Law 88-19 (Law N 88-19, 1988) marked the beginning of the law under this category entitled “computer crimes”. Followed by the law 92-683 (Law N 92-683, 1992) which contained amendments to the penal code. Followed by another law 2004-575 (Law N 2004-575, 2004) that was about confidence in terms of the information economy. To sum up, we find no clear definition of digital crime in the articles of the above-mentioned laws. Where it only provides superficial examples about the

offenses that are classified under the category of digital crime mainly the ones like illegal login in the automated data processing system.

Arabic legislators also defined digital crime. The latter is defined according to the Saudi legislator as "any act that involves the use of a computer or any other information network in the violation of the provisions of these regulations (Saudi System of fighting digital crime, 2007). Where we find clear limits on the offenses of digital crime using the computer and the Internet. Moreover, the offense should be listed in the provisions of the cybercrime control system.

Whereas according to the Syrian legislator digital crime is defined as,"any offense committed using computer devices or networks (Syrian law on the regulation of networking and fighting against cybercrime, 2012) Like the Saudi legislator the Syrian, one also limits the acts under digital crime. Unlike the Egyptian legislator, which gave a more broad definition for this concept in that it is defined as any act or offense committed through an electronic broker (Bachir, 2020 2021, p. 11).

2- **Judiciary definition of Digital Crime:**

The Judiciary definition of digital crime is completely different from the legal one due to its absence in the country's legislation. Many definitions appeared without being able to reach one agreed definition as if the digital crime is unknown.

According to Merwe, digital crime is an illegal offense committed through a computer. Or any criminal offense where information programs are used as the main tool (Azizi. Khedri, 2020. P3)Whereas others define it as acts committed through information networks (Lizi, 2022, P542).

Klaus Tieduman defines it as the unlawful conduct committed using a computer (Aziz, Khdri, 2020, P 3).

The organization of economic cooperation and development (OECD) defined digital crime as any act or omission that would infringe material and moral funds which are caused by the interference of information technology directly or indirectly (Ammimer, 2021, P 13). To sum up, all the above-mentioned definitions focused on the tools used to commit this act.

What can be deduced from these definitions is that digital crime is restricted in one case, which is the use of computers and information networks. However, what if this crime was committed on a computer or an information network?

Others like Blat Ros define digital crime as an unlawful activity used to paste, change or delete access to information stored on a computer .(Azizi, Khedri, 2020, P 3) Moreover, it is also defined as a negative or positive behavior directed towards violating programs or information for various purposes. (Yermech, 2020-2021, P18)

While defining digital crime, a lot of them relied on information technology knowledge. Because this type of crime requires technical experience (Ghernaouti, 2018, P11) in the domain of information knowledge technology. However, in reality, those who lack technical experience or those who do not have enough knowledge of computer techniques commit digital crimes. Hence, technical knowledge is not a must or condition in this crime. Following the definitions that are mentioned previously, we can define digital crime as any illegal activity committed in a digital environment using an information base directed towards violating it for various purposes.

Paragraph 2: Characteristics of Digital Crime.

Digital crime and conventional one are extremely different this mainly lies in the digital environment where those crimes are committed.

1-Difficulties in proving Digital Crime.

Unlike conventional crimes, digital crimes are committed in a few seconds (Al Hussaini, Marey, 2019, P 31) unlike conventional crimes where effort is required for crimes like stealing or killing. One of the characteristics of digital crime is that it lacks the violence and noise or chaos that are resulted from conventional crime.

Due to the lack of evidence, it is difficult to prove digital crimes because perpetrators are so tricky in terms of hiding evidence. Which makes the work of traditional investigators even more complicated. Add to this deception is the main issue in digital crimes ,(Attouch Al Mouach, 2017, P 30)What makes the proving process even more difficult is the virtual setting where this crime is committed. This led to missing many crimes due to the absence of a geographical setting (Mouchtag, 2014, P 345)that would facilitate the identification of perpetrators.

2-Digital Crime is transnational and causes extreme damages.

Geographical borders are not considered in information societies. Because the location is not an issue for networks,alternatively the latter do not rely on a specific place or period of time (Al Moumni, 2010, P 50), in other terms it is not subject to borders control. The Internet played a significant role in digital crimes. Communication became much easier, despite the distances that exist between the users. Exchanging and transforming information became an easy task. Talking about the disadvantages of this gradual progress on the internet so many countries are and will be affected by digital crimes (Matoug, 2011-2012 ,P 14).

Digital crime causes various damages to victims. Where it is difficult to value them. This can be summarized into the following: the spread of destructive viruses, and spying over the private life of people. Add to this the national and the political security of many countries is affected by this type of crime (Al Nouaizza, 2017, P79).

Second Requirement: Motives of Digital Crime and privacy of its parties.

Digital crime is similar to conventional crime in that it has two parties; the perpetrator and the victim. Research shows that the parties involved in digital crime are completely different which will be emphasized in section 1. Concerning the motives will be presented in section 2.

Paragraph1 : Privacy of the parties of Digital Crime.

1- Perpetrator in Digital Crime.

Parties involved in digital crimes are so special this gives them specific characteristics, which will be explained below; Perpetrators of digital crime are normal people who possess considerable knowledge about computers. Unless perpetrators are helped by those who are more skilled in computer science (Al M anaasa, Al Zouebi, 2014, P75). Digital perpetrators are more skilled in terms of adapting to their social environments. Add to this, they are more confident in their work setting. Moreover, they do not show themselves as enemies to their surroundings they are more agreed with them (Rabie, 2015-2016, P 35).

According to jurisprudence, perpetrators of digital crime are divided into four categories. The first category refers to youngsters who commit crimes unintentionally. Add to this they commit it with good intent, they are not knowledgeable about the penalties of those crimes. Moreover, we find also workers in the field of computers who take advantage of their jobs (Al Manaasa, Al Zouebi, 2014, P78). The third category is about those who are experienced and skillful mainly having criminal attitudes and tendencies aiming to vandalize (Saghir, 2013, P 27). They are characterized by their desire to know more about the digital environment, which enables them to violate security borders, which reflects their intelligence in terms of computers and networks.

2- **Victims in Digital Crime.**

Victims of digital crimes are numerous they could be business companies, governmental institutions, and normal individuals. However, this type of crime is widely recognized in sectors that rely heavily on computers for their services.

One of them is bank sectors due to the excessive usage of the internet. Add to this, industrial production sectors (Al Manaasa ,Al Zoubei, 2014, P 81). Another category that falls into the trap of digital crime is children who use electronic mailing, which happens through daily messages that they receive with a percentage of 80% (Tamam, 2019, P 25). Where they receive emails about their images and even receive threats because of this. Digital crime is also spread in military sectors through spying over data and trafficking it (Al Manaasa, Al Zouebi, 2014, P 81). An important idea that should be considered here is that victims in digital crime play a significant role, unlike conventional crimes where victims prefer to cover up the truth especially if it is an institution or a company to protect their relationships with their agents.

Paragraph 2 : Motives of Digital Crime.

Like any crime, money is the first motive. Digital crime perpetrators have their motives, which are different. They will be presented on the following points:

1- **Personal motives.**

This is mainly linked to the perpetrator`s personality they are summarized in the following:

-Challenging the information system:

This is mainly done to show their ability in overcoming the digital systems no matter how developed they are. This aims to show their capacities in breaking down the demonstrating security barriers of digital systems (Al Moumni, 2010, P 92). This takes the form of challenges between perpetrators themselves to show their capacities to break down any system at any time, which makes them have fun while doing this.

-Desire to Learn: this enables perpetrators to be updated about the last techniques in the digital world. Allowing them to spend more time on computers to unlock their hidden features.

-Revenge: this is considered a strong motive mainly committed by the workers over their directors or bosses (Al Nouaizza, 2017, P 88).

2- **External motives.**

-Political and military motives: an example of this is what the Russian pirates have done over American computers for over a year where they have stolen sensitive data but are not that secret (Chantir, 2020-2021, P 37), Add to this the excessive use of digital tools maximizes the chances of digital crime due to the sensitivity and the important role that the sector holds.

-Trade competition: this is mainly between competing companies making them an easy target for hacking at any moment.

SECTIONII : PROVING DIGITAL CRIME.

As mentioned earlier it is very difficult to prove digital crime due to the absence of concrete proofs or evidence. Proving this type of crime requires highly developed tools and techniques that match its progress. Because traditional tools are unable to prove this. This section will provide an overview of traditional procedures (1) followed by modern procedures (2).

First Requirement: Classical procedures for proving digital crime.

Those procedures or techniques are more appropriate in conventional crimes; however, we can rely on them in digital crimes which are divided into physical and personal ones.

Paragraph1 : Physical mechanisms in proving digital crime.

Those mechanisms do not show the personal element where they rely heavily on physical work; they do not require any special characteristics in the doer. They are mainly inspection and verification.

1- **Inspection.**

Investigators must carry out inspections so they can identify perpetrators of digital crimes. Which requires a login to the information system looking for evidence. This infringes the privacy of the accused person (Ben Ferdia, 2015, P 128). This definition matches exactly conventional crimes in terms of looking for concrete proof. According to the European Council, inspection is definedas: a procedure aiming to collect stored or data registered electronically through the use of electronic devices (Ben Ferdia, 2015, P 128).

Jurisprudential views differ concerning the possibility of carrying out inspections in digital crime because the latter is found in information systems, which have physical and moral elements.

When talking about physical elements this takes the form of the computer like the solid memory, electronic processors, cables, keyboard, and printers (Madjdoub, 2019, P 111). Inspection carried over those elements is dependent on the nature of the place either public or private setting. Where the setting plays a vital role in the inspection process (Ben Taleb, 2017, P 489). When carrying out the process of inspection of physical objects it is necessary to obey the rules set by the law.

As for the abstract elements of the computer, this has been debated. This debate has its advocates who call for the inspection of concrete elements. Whereas for opponents who are against the process of inspection. This issue has been resolved by the Algerian legislator, which is emphasized in articles 5 from 09-04 law which allows access aiming to inspect including virtual settings of information systems or part of it in addition to that data that is stored in it.

2- **Verification.**

Verification plays a vital role in proving the digital crime. Through searching the crime scene. According to article 79: order 66-155 (Order 155-66, 1966) the investigating judge should visit crime scenes to conduct the necessary verifications. This could be carried out in conventional crimes that are committed in concrete environments where traces could be left for verification.

However, when it comes to digital crimes the crime scene differs. Crime scenes in digital crime are computers, numerical data,and hard drives. The process of verification in digital crimes consists of looking for any fingerprints or traces that are left by the network users or the internet. The latter gathers all the sent and received messages and all electronic calls (Chantir, 2020-2021 P 64). Add to this verification in digital crime could be carried out virtually without the need to move to the crime scene, However, verification is guided by regulations, which are stated above:

Take pictures of the computer and its accessories and the different cables that are linked to it.

Protecting saved data from damage.

Saving specific documents/ folders with a careful check-up for fingerprints that they may contain like magnetic disks.

Looking after the settings of the computer and its operating programs and the type of automated processing system for information. In addition, whether or not the computer is connected to the internet (Matoug, 2011-2012 ,P 109). What can be deduced is that proofs of digital crimes are rarely left behind add to this they are destroyed to hide the truth.

Paragraph 2 : Personal mechanisms for proving Digital Crime.

This requires the presence of a qualified person. This is mainly about technical expertise and certification.

1-Technical expertise.

When it comes to digital crimes, technical expertise is necessary for that it helps to reveal the truth. Due to the nature of this crime, as well, as the computer information systems that are used moreover the internet; this all demands experts with special skills.

Technical expertise is one of the procedures that is carried out by someone who has technical capabilities and scientific qualifications which are absent from the investigation and judiciary sectors, aiming to discover evidence that helps in revealing the truth depending on the type of the crime and those who are accused (Brahimi, 2018, P68). Technical expertise plays a vital role in digital crime in that its absence or assigning it to those who are less qualified would result in damage to the proofs which are required when dealing with the different techniques of information.

Article 143, article 156 from the code of criminal procedures is specified for organizing the tasks of technical expertise which was an issue that has been the focus of the Algerian legislator. Due to the pivotal role, it plays in digital crime where this has been included in specific laws. Where an establishment of the expertise department for technological manuals of the technical section of the National Institute of investigation science has been established (Article 5, 2007).

Article 5 from laws 4-9 mentioned above enables assigned authorities to carry out inspections by those who possess knowledge or are more knowledgeable about the way information systems work by providing it with the necessary information that would help. Article 13 from the same law states the establishment of the National committee that protects from crimes linked to information and communication technologies and fighting against it. Its tasks are listed in article 14: it handles and enables judicial authorities and judicial police in the process of investigation that is carried out about crimes that have relation to information and communication technologies including the collection of information and achieving judiciary expertise which all require the presence of technical experts in the domain of digital crime.

2- **Testimony.**

Testimony is an important step in criminal proving (Ben Ferdia, 2015, P 151). Unlike writing which is a vital tool in civil proving. Unlike conventional crimes where finding a witness is considered an easing way for justice. Digital crime witnesses are very hard to find. This is because the settings of the crime differ. Add to this victims are prevented from reporting. Generally, the witness in digital crimes differs totally from the ones in conventional crimes.

The witness in digital crime is called an information witness. They should be experts and specialized in computer communication network techniques. This is so crucial for logging in to the automated data processing system if an investigation requires looking for criminal proof inside the system (Hbibatny, 2020, P350). Information witnesses are mainly computer operators' price programming experts, maintenance and communication engineers, and analysts' system managers. What should be clarified here is that an information witness is not the same as a technical expert. The two are different. The first is required to testify based on information he may have heard or seen. Whereas the second task is to prepare an expert report according to or based on technical and scientific standards.

Second Requirement: Modern procedural mechanisms for proving digital crime.

Due to the mysterious characteristics of digital crime in addition to the rapid development of the means of committing it. Conventional procedures failed in detecting and looking for proof. Which results in missing criminals. This in turn requires the urge to develop procedures that are more advanced and effective.

The Algerian legislator issued the law 06-22 (Order 06-22, 2006) which emphasizes the procedures that Have been developed and followed by modern procedures found in law09-04 (Law 09-04, 2009) section two.

Paragraph1 : developed procedures law 06-22.

Which takes the form of interception mechanisms of correspondence،recording voices, taking pictures as well leakage mechanisms.

1-Interception of correspondence.

recording voices, taking a picture One/ Interception of correspondence: recording voices taking pictures, interruption of messaging.

This has been included in the Algerian legislator in law 22-06 article 65 bis 5. Until article 65 bis 10. In chapter four under the heading, "interception of correspondence, taking pictures, recording voices. According to article 65 bis 5. It is required to investigate committed crimes(that are suspected)including crimes or offenses related to automated data processing systems where it is allowed for the republic prosecutor the specified one to prevent messaging which

occurs through telecommunication tools through setting the technical preparations aiming to capture, install, record conversations or taking pictures for one person or groups of people who are found in a special place (location). This is clearly illustrated in this article that the type of messaging that can interrupt are those done through telecommunication means.

Not mentioning the types of messaging that require interruption or that could be interrupted gives it open access to all the writings despite its types (writings, symbols, shapes, photos) either being written or digital or how this is done or used in sending it like: fax, telegram, or electronic mailing, cell phones) (Yermech, 2020-2021, P174).

The French legislator allowed the investigating judge to follow this procedure if it is required during an investigation found in the code of criminal procedures.

Le juge d'instruction peut, lorsque les nécessités de l'information l'exigent, prescrire l'interception, l'enregistrement et la transcription de correspondances émises par la voie des communications électroniques (Article 100, 2022).

Recording voices (audios) and taking pictures become much easier due to the progress and the development of technological tools. The latter is permitted or allowed by the legislator according to technical preparations and without the consent of the concerned.

The process of recording voices according to the above-mentioned article means saving talks (conversations) secretly by one person or a group of people in public or private places. Whereas taking pictures is about installing someone`s pictures on a platform specified for its purpose.

2-Information leakage.

The latter is also called: hacking. This is mainly found in chapter five. Law 06-22 article 65 bis 11, until article 65 bis 18. Hacking is defined according to article 65bis 12 as a process done by a judicial police officer or assistant under the responsibility of the judicial police officer which focuses on supervising members suspected of having committed a crime or a misdemeanor. The officer responsible for this or in charge of this should play the role that he is with or in other words involved in the crime. Therefore, this makes it even more complicated. The success depends on the high skills of the officer in hiding their real identities and playing their roles perfectly.

In digital crimes people in charge of the leakage process of leakage hack certain websites and open various electronic gaps. They even participate in chatting groups with suspects and more importantly, they should show themselves as being involved with them so they could benefit from their knowledge in hacking websites (Saidani, 2012-2013, P 177).

The leakage process could not proceed unless permission is obtained from the republic prosecutor and the investigative judge, which is clearly stated in article 65. Bis 11. Another condition, permission should be written and justified which is clearly stated in article 65 bis15.

Where oral permission is rejected and not accepted. The leakage process should not proceed for four months with the possibility of renewing it according to the demands, or in other words the requirements of the investigation. Moreover, can stop this process at any time if the period is still valid.

The success of this process is dependent on not showing the real identity and hiding it. So according to article 65: bis 16: whoever tries to share information about this process will be imprisoned for 2 to 5 years. Moreover, paying a fee of 50,000DA to 200,000 DA.

Paragraph 2 : Created procedures according to law 09-04.

This takes the form of electronic monitoring mechanisms. In addition to information data seizure; which will be explained below:

1-Electronic monitoring.

according to article 3 from the law 09-04 that according to the requirements of ongoing judiciary inquiries and investigations are allowed to organize the technical preparations to monitor electronic calls and record their consent. However, when it comes to the meaning of this technique then the legislator did not give its definition where it only specifies electronic calls in article2. In that, it is about sending, receiving signs, writings, pictures, or voices of different information through any electronic medium or tool.

According to jurisdiction, the latter is defined as a task carried by a monitor/watcher, an observer using an electronic technique aiming to collect and gather data and information about suspects. Suspects could be a person or group of people or a given location (setting) or anything, depending on its nature linked to time which aims to achieve a security purpose or any other purpose (Saidani, 2012-20,13 P183).

Electronic monitoring is not only used as a proving procedure, however; it can be used as a protective tool practiced before the occurrence of this type of crime. Where in article 4 the same law the above-mentioned procedure could be initiated in case of the possibility of any threat that would destroy public order, national defense, state institutions, or national economy.

Equipment that is used in electronic monitoring is the following the computer or any website in a given connexion network which includes electronic messages, discussion circles, chat rooms which can be carried by a cell phone connected to the internet, electronic watches, and tablets (Moulay Meliani, 2018-2019, P209). To sum up it can be found in any electronic device connected to the internet and electronic communication despite its types, which have already been defined.

Electronic monitoring is considered a very serious procedure. The reason is that it immerses itself in private life; moreover, it looks at the rights that have been put by the laws and constitutions. Therefore, the latter is organized by conditions according to article4 law 09-04. Electronic

monitoring can be carried out in the presence of written permission issued by the competent judiciary authority also; it could be carried out in case of difficulties in reaching results about the investigation without electronic monitoring.

Seizure of electronic data.

The seizure of electronic data has been debated whether to be seized or not unlike the seizure of physical objects. This has been clearly stated in law 09-04 from articles 6 -9 which emphasizes how electronic data can be seized:

First, one is about pasting: according to article 6: when data are discovered while carrying out an investigation, and the latter is helpful in the process or when the authority starts looking in information systems and stored data are detected which may help in crimes and looking for suspects and not all data should be seized. Only those that facilitate the investigation could be seized. This process is carried out on an electronic storage base, which also can be seized and put into attachments.

The legislator introduced or modernized this procedure in parallel with article 19 section 4 of the Budapest convention: which state the following each authority in a given country to follow the following procedures: to control computer systems or part of it. Alternatively, information stored on any medium and to protect the stored information (Amimer, 2019-2020, P302).

Whereas the second way refers to seizure through blocking access to data, which is stated in article 7: which states the following if the seizure is inaccessible according to regulations stated in article 6 for any technical issue. Then it is the authorities' task to carry inspection to use the appropriate techniques to block or prevent access to data that is found in the information system or to copy it by those who are authorized to do this.

The process is done through the appropriate technical tools to prevent access to data of the information system, which is part of the crime or contains proof about it. Aiming to protect data in its electronic space and to prevent any trials of hiding the truth (El Baraka, 2020-2021, PP 295, 296). Through article 8 the legislator allowed the authorized authority to carry out an inspection to follow the appropriate procedures to prevent access to data related to crimes. By giving this task to a skilled person, who is knowledgeable about the appropriate techniques. Like preventing access to pornographic websites as well terrorists that spread misleading ideas and explaining ways of making bombs and so forth (Moulay Meliani, 2018-2019, P243).

Conclusion:

To conclude the process of proving digital crime is so crucial and plays a significant role in fighting against this crime. The proving process depends on the use of the appropriate procedures that match the digital crime. The Algerian legislator worked hard in terms of issuing laws that fight this type of crime. Many of these laws contain modern procedures that match the

development of digital crime. Without ignoring the classical mechanisms that helped in proving this crime. The following includes recommendations that have been reached out:

The need to prepare security agents through training in the field of information systems who would be professional in dealing with digital crimes.

The need to gather digital crime texts in a dependent law that should contain information about investigation mechanisms and search mechanisms specific for this crime.

Bibliography List setting:

Books:

-Abdelilah Mohammed Al Nouwaissa (2017) Information technology crimes explanation of substantive provisions in the law of electronic crimes, 1st edition, House of Wael for publication and distribution, Jordan.

-Adel Hamed Bachir, (2020-2021), Criminal proving of electronic crime, 1st edition, House of Arabic Renaissance, Cairo.

-Abdelkader Amimer, (2021), Legal challenges for proving electronic crim, University House for publication, Algiers.

-Chawki Yaayich Tamam, (2019), Electronic crime, comparative study, 1st edition , El Rimal press, El wadi, Algiers.

-Dergham Djebbar Attouch Al Mawach (2017), Information spying crime, comparative study, 1st edition, Arabic center for distribution and publication, Republic of Egypt.

-Nessrine Mouhssen Nimat Al Houssain, Mohammed Hassan Marei (2019), Electronic crimes over money, 1st edition, Modern university Bureau, Egypt.

-Oussama Ahmed El Manaasa, Djalal Mohammed Al Zouebi (2014), information systems technology crimes, comparative study, 2nd edition, House of culture for distribution and publication, Jordan.

-Solange Ghernaouti, (2018), la cybercriminalité, les nouvelles armes de pouvoir, 2eme édition, ITCIS, Algiers.

Theses:

Ph.D. Dissertations:

-Abdelkader Amimer, (2019-2020), procedures for proving electronic crime in the Algerian legislation, comparative study, faculty of law, University of Algiers 1, Algiers.

-Al Taibi Al Baraka, (2020-2021), Criminal protection of the automated data processing system, comparative study, faculty of legal and political sciences, University of Ahmed Draya, Adrar, Algiers.

-Ben Ferdia Mohammed, (2015), criminal proving with digital evidence for electronic crime, faculty of law, University of Algiers 1, Algiers.

-Brahimi Djamal, (2018), criminal investigation in electronic crimes, thesis, faculty of legal and political sciences, University of Mouloud Maameri Tizi Ouzou, Algiers.

-Chentir Khedra, (2020-2021), legal mechanisms for proving electronic crime, comparative study, faculty of legal and political sciences, university of Ahmed Draya, Adrar, Algiers.

-Hbibatny Bouthaina, (2020), crime related to information and communication technologies, Faculty of law, university of Algiers 1, Algiers.

-Moulay Meliani Dalal, (2017-2018), the issue of proving internet-related crimes in the Algerian legislation, faculty of legal and political sciences, University of Abu Bakr Belgaid, Tlemcen, Algiers.

-Rbaiy Houssain, (2015,2016), Investigation and search mechanisms in electronic crimes, Faculty of Legal and political sciences, University of Batna 1, Algiers.

-Yermech Mourad, (2020-2021), the specificity of electronic crime, Faculty of Law, University of Algiers 1, Algiers.

Master Thesis

-Maatoug Abdelatif, (2011-2012), the legal framework for combating electronic crimes in the Algerian and comparative legislation, faculty of legal and political sciences, university of Colonel Al Hadj Lakhdar, Batna, Algiers.

-Saidani, Naiim, (2012-2013), Investigation and searching mechanisms of the electronic crime in the Algerian Law, faculty of Legal and political sciences, University of Al Hadj Lakhdar, Batna, , Algiers.

-Sghir Youcef, (2013), crime committed through the Internet, Faculty of legal and political sciences, university of Mouloud Maameri, Tizi Ouzou, Algiers.

Journal article:

-Lynda Bentaleb, (2017), inspection in electronic crime, Magazine of Legal and political sciences, University of Echahid Hamma Lakhdar, El Oued, number 16, pages 489.

-Lamia Madjdoub, (2019), Inspection procedure in electronic Fraud, Journal of communication in Economics, Administration and Law, University of badji mokhtar, anaba, number 3, pages 111.

- Mouchtag Taleb Wahib, (2014), the concept of electronic crime and the role of the computer in committing it, magazine for legal and political sciences, University of Diyala, number 1, pages 30-345.

-NASSIMA AZIZI, IBTISSEM KHEDRI, (2020), cybercriminalité, un fléau planétaire, revue DIAA des études juridique, centre universitaire Nour Bachir El Bayadh, numéro 1, pages 3.

-SAID LIZI, (2022), la cybercriminalité, réalité et défis, Journal, Researcher for Legal and Judicial Studies and Research number 1, pages 542.

Legal Texts:

-Law N: 04-15 of10th November 2004, amending and supplementing the order N: 66-156. Issued on 8 June 1966, including the penal code, official journal. Volume 71of 10th November 2004.

-Law N 06-22 of 20th December 2006 amending and completing order N: 155-66 OF 8th June 1966, including the penal code of criminal procedure, official journal N 84 of 24th December 2006.

-Law N: 09-04 of 5th August 2009, including the specific regulations of preventing crimes related to information and communication technologies, officialjournal, issue 47, issued on 16 August 2009.

- Order N 66-155 issued on 8th June 1966, including the code of criminal procedure, official journal, volume 48, issued 10th June 1966.

-Joint Ministerial decision of 14th April 2007, concerning the organization of regional departments, interests, and laboratories of the National institute for research in criminal investigation sciences, official journal, volume N 36 of 3rd June 2007.

-Saudi computer crime control system of 27-3-2007.

-The Syrian law on regulating networking and fighting electronic crime, issued by the legislative decree N 17 of 2012.

- Code procédure pénale français, dernière modification 01-05-2022.

- Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique, journal officiel français du 6 janvier 1988.

- Loi n^0 92-683 du 22 juillet 1992 portant réforme dispositions générales du code pénal, journal officiel français du 23 juillet 1992.

- Loi n^0 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique , journal officiel français du 21 juin 2004.