PSYCHOLOGY AND EDUCATION (2021) 58(5): 6784-6797
ISSN: 1553-6939

Inspection and seizure as a means of collecting evidence in information crime

Prof. DrNaserKramishKhuder, M. Nibras Abdul KadhimWeni

College of Law,DhiQar University, Ministry of Higher Education and Scientific Research,The Republic of Iraq

Emails: lawp1e207@utq.edu.iqLaw6phd13@utq.edu.iq

Abstract

The information crime is one of the most complex and most dangerous crimes, due to the special characteristics of this crime in terms of the methods of committing it, its modernity, characteristics and the characteristics of the criminals who carry it out, in addition to the difficulties that this type of crime raises at the procedural level, as most of the texts of the procedural laws were formulated To address traditional crimes in which there are no difficulties facing the investigative authorities in the field of investigating and proving them and collecting evidence obtained from them, while we find the insufficiency of such procedures in investigation, proof and evidence collection in information crimes, which made some countries to urge their legislators to make special legislation To address and regulate information crimes in addition to its traditional punitive legislation, and this is what the Iraqi legislator directed to in the Iraqi Information Crimes Project for the year 2011, as an attempt to equalize what many countries went to in this field.

technology means and the increasing reliance on it, foremost of which is the Internet. The private lives of individuals were the reason for causing huge losses to the economies of countries in that the criminal found modern methods that enabled him to commit his crime without leaving traces that would help in its detection, and this is what placed on the competent legal authorities serious difficulties that exceed their capabilities available to them in the field of investigation. And collecting evidence in traditional crimes, which are usually limited to confronting

The Introduction

The Industrial Revolution played a key role in paving the way for a new revolution, namely the information revolution, which had a significant impact on changing the lives of individuals in many areas due to the speed and accuracy of information technology in processing and exchanging data and information, whether within the state between individuals and institutions or outside the state. Within the framework of international relations, but with the expansion of the use of information

on information crimes for a number of countries.

Research Structure:

In order to become familiar with the subject of the study, we decided to divide the research into two sections. In the first section, we deal with the nature of the information crime, and it has two demands. The first requirement defines the information crime, and in the second requirement is the characteristics of the information crime and the characteristics of the information criminal. As for the second topic, it will be devoted to inspection and control in the information crime and is divided into two demands. The first requirement is devoted to inspection. In the information crime and the second requirement, we will deal with the control of the information crime.

This is followed by a conclusion that includes a recording of the most important results and recommendations that we reached through this research.

Unit one

What is information crime?

The emergence and development of the Internet in this wide and steady form, and the increase in the number of users of the electronic network in the world, made the Internet a suitable medium for planning and implementing a number of crimes away from the control and eyes of the security authorities. The rapid pace of technological and technological progress, the emergence of cyberspace information crimes that may fall on certain funds It is an intangible state, and this is what we do not find in the context of traditional crimes that are not replaced by material funds.

Research Importance :

The importance of the topic is by considering information crimes as one of the modern topics that raise many difficulties in the field of criminal proof, as well as the connection of this topic to the development of modern electronic means, which is reflected in the development of methods of committing this type of crime.

Research Problem:

The problematic of the subject under research is about the adequacy of the procedures and means of collecting evidence used in traditional crimes to confront information crimes that are committed in an intangible virtual scene that is completely different from the traditional crime scene, in addition to the nature of the place of these crimes, which has a moral and immaterial nature, and from the nature of the crime Informatics is a cross-border crime whose effects may extend across countries, and this raises the problem of proving it.

Research Methodology :

The research is based on extrapolation and analysis of the texts of the Iraqi Information Crimes Bill of 2011 and the Iraqi Criminal Procedure Code No. (23) of 1971, compared to some traditional legislation and legislation

from the perpetrators of traditional crimes, we will divide this unit into two demands.

In the first requirement, we deal with the definition of the information crime, and we dedicate the second requirement to the characteristics of the information crime and the characteristics of the information criminal.

The first requirement

Definition of information crime

Before delving into the jurisprudential and legal definitions of information crime, it must be pointed out that there is no agreement at the doctrinal and legislative level on a specific term to denote this newly created criminal phenomenon. Modern technology crimes." As for the prevailing opinion, with which we agree in the nomenclature, it is those who prefer to use the term "information crime" over crimes related to the computer and the Internet.Each attack includes various forms of information technology.

As for the definition of information crime as a jurisprudence, the jurisprudence did not agree on a comprehensive definition of information crimes due to the absence of a unified legal term to denote the crimes arising from the illegal exploitation and use of information technology, as we indicated at the beginning of the research.

Therefore, jurisprudence tried to find a definition of information crime, and it was divided into three directions:

and modern means of communication such as fax, the Internet and other forms of electronic communication via satellite, have been exploited by the perpetrators of electronic crimes in the implementation of their crimes, which are no longer confined to the territory of one country, but transcend the borders of states, and they are innovative and novel crimes that represent a kind of Types of criminal intelligence have been difficult to include within the traditional criminal descriptions in national and foreign criminal laws, at a time when technology, for example, has brought distances between peoples closer, by providing many means of communication and means of transportation that were not known before (such as the Internet) and the information network. We find that this technology has produced many negatives, perhaps the most important of which was the difficulty of maintaining one's privacy due to the spread of many easy means, which are used by people known as hackers of the Internet and through which they break into the privacy of the individual Against his will, or assault people through a Using this information network for insults, slander, defamation and other acts criminalized by law.

In order to understand the nature of the information crime by defining the term information crime, and to clarify the most important characteristics that characterize it and the characteristics of its perpetrator that distinguish it

that may be punishable," as it defined "a group of crimes related to the science of processing." Logical Informatics[4]

As for the definition of information crime legally, we find that some legislations have defined it. We mention from that the American legislator in the Computer Crimes Law No. (1213) for the year 1986, where he defined it as "the unauthorized use of protected computer systems or data files, or the intentional harmful use of computers or data files." [5]

As for the Saudi legislator, the information crime was defined in Article (18) of the Saudi Information Crime Control Law No. (17) for the year 1428 by the text "any act committed involving the use of a computer or information network in violation of the provisions of this system".

As for some other legislations, we find that they dealt with the provisions of information crimes, but they did not provide a specific definition in their texts, including the Law on Combating Information Technology Crimes for the year 2018 in Egypt, as well as the Iraqi draft law on information crimes for the year 2011, which contented itself with clarifying the provisions of information crimes in terms of definitions and objectives in the

4. Dr. Hoda Hamed Qashqoush, Computer Crimes in Comparative Legislation, Dar Al-Nahda Al-Arabiya, Cairo, 1992, p. 8.
5. Rami Metwally Al-Qadi, Combating Information Crimes, Dar Al-Nahda Al-Arabiya, Cairo, 2011, p. 23.

The first direction: defined it from the information and electronic data itself, as he defined it as "an illegal activity directed at copying, accessing, changing, deleting, or diverting information stored inside electronic devices."

The second direction: defines it based on the means that is used to commit it, as it is stated as: "Every criminal act that uses an electronic device to complete it[1].

The third direction: which combines the two previous trends, which are the objective trend that stems from data and information, and the third trend that stems from the means by which electronic crime is committed, as he defined it as: "Every intentional act or omission that arises from the illegal use of information technology and aims to Assault on material or moral funds[2].

Among the other jurisprudential definitions that were said in the definition of information crime, we mention its definition as "legal attacks that are committed by means of information technology with the aim of making a profit."[3] And the information crime was also defined as "a group of acts related to information technology

1. Osama Ahmed Al-Manasah, Information Technology Crimes, 1st Edition, Wael Publishing, Jordan, Amman, 2001, p. 73.
2. Muhammad Ali El-Dian, Cybercrime, New University, Alexandria, 2011, p. 56.
3. Saad Al-Hajj Bakri, Communication Networks and the Employment of Information in Combating Crime, The Arab Journal for Security Studies and Training, p. 6, p. 11, Riyadh, 1990, p. 92

First section

Characteristics of information crime

The association of information crime with electronic devices, whether these devices are the means of this crime or its place, makes it have characteristics that distinguish it from the traditional crime and give it a special character, which we mention as follows:

1- The small number of cases that have already been discovered compared to what is discovered from traditional crimes, and if the information crime is discovered, it is sometimes a coincidence [7]

2- The information crime is not characterized by the violence that characterizes other traditional crimes, to the extent that it is said that there is no real feeling of insecurity in the face of information crime as there is always in the face of other crimes. The traditional image of the criminal almost disappears in these crimes. On the contrary, the information criminal usually belongs to a higher social level than other criminals, and he is rarely a professional criminal or a returnee, and he is not seen as a criminal in the common sense of this word.

3- Absence of a general feeling of immorality of the act or prejudice to the interests and values that society is keen to protect. Indeed, many workers in the field of informatics do not find any embarrassment in using codes and chapter The first of it and the punitive provisions in the second chapter, which included many information crimes, including crimes against the internal and external security of the state, terrorist crimes, some crimes related to the specific and comprehensive jurisdiction of criminal law, crimes of theft of information and electronic data, crimes of electronic forgery, crimes of destroying electronic data and other crimes, as for the third chapter. It was devoted to evidence collection procedures, which is what we will explain in the second section of the research, and it also included investigation and trial procedures, and finally, the fourth chapter came with general and final provisions[6] .

The second requirement

Characteristics and the characteristics of a cybercriminals and crim

In this requirement, we will address the statement of the characteristics that characterize the information crime, as well as the characteristics that its perpetrator enjoys that distinguishes it from the perpetrator of the traditional crime, in two branches, as follows:

7. Jamil Abdel-Baqi Al-Saghir, Criminal Law and Modern Technology, 1st Edition, Dar Al-Nahda Al-Arabiya, Cairo, 1992, p. 17

6. The Organization for Economic Cooperation (OECD) for the Information Fraud Questionnaire in 1982, which was mentioned by Belgium in its report, defined that cybercrime is “every act or omission that would attack material and moral funds, resulting directly or indirectly from the intervention of information technology.”

second section

Attributes of a cybercriminal

A cyber criminal is a person with skill, knowledge, and intelligence, and when he commits a crime, he justifies it with different justifications because he is afraid of revealing his crime. One of the motives that drives the information criminal is a person with skill, knowledge and intelligence, and when he commits a crime, he justifies it with different justifications because he is afraid of revealing his crime. Among the motives that drive the information criminal to commit a crime are the desire to learn, conquer the information system, prove oneself, and the desire for revenge, fun and challenge. There are material motives such as profit and making money, and there are other motives such as political and economic competition and military competition between countries. The information criminal to commit a crime desire to learn and conquer the system. There are material motives such as profit and making money, and there are other motives such as political and economic competition and military competition between countries[9].

1- The perpetrator of cybercrime is mostly an intelligent and cunning person with high technical skills and familiarity with the method used in the field of computer systems and how to operate it and how to store and obtain information, while the perpetrator of illegally entering into computer systems.

4- The information crime takes place in the field of automated processing of information and targets morale, not material, and is therefore less violent and more difficult to prove because the perpetrator of this crime does not leave behind any tangible external material trace that can be examined, and thus the victim is sometimes not aware of the occurrence of the crime because The offender usually has the ability to block the behavior that constitutes the crime by adopting methods that would manipulate the electronic vibrations through which the data is recorded[8]. Getting to the truth.

5- The information crime has an international dimension, that is, it is cross-border, as it may exceed geographical borders, considering that its implementation is carried out through the information network, and therefore the multiplicity of places related to crime and the conflict of laws of applicable countries in addition to the difference in criminal procedures from one state to another, which raises the Oftentimes, legal, administrative, technical, and even political challenges are faced, especially with regard to criminal prosecution procedures.

9. Nahla Abdel-Qader Al-Momani, Information Crimes, 1st Edition, Dar Al-Taqqa, 2008, p. 77.

8. Khalil Youssef Jundi, Legislative confrontation of information crime at the international and national levels, research published in the Journal of the College of Law for Legal and Political Sciences, No. 26, Volume 7, 2018, p. 92

the competent judicial authorities and their smart methods in wasting evidence resulting from their crimes[11]

Unit two

Inspection and seizure in information crime

Evidence-gathering means are a set of actions that the competent authority considers appropriate to carry out to reveal the truth regarding a specific incident of interest in the Penal Code. The means or procedures for collecting evidence are not exclusively mentioned in the law. Therefore, the competent authority may initiate any other procedure that it deems useful for evidence as long as it does not result in a restriction of the freedoms of individuals or a prejudicial to their private lives.

Since the illegal use of computer technology and the Internet has caused many procedural problems in the field of criminal prosecution procedures that are followed in order to detect the crime and establish evidence of its occurrence and attribute it to the perpetrators who use advanced technology to commit it and to conceal its features and not leave any material traces indicative of it, all This led to the intervention of the legislators of some countries to confront this type of crime by issuing special laws to prosecute them and organize the procedures that suit them without the traditional crime is mostly a person of average education.

2- The perpetrator of the cyber crime is mostly socially adapted and financially able, motivated by the desire to conquer the system more than the desire to obtain profit or material benefit, while the perpetrator of the traditional crime is often socially unadapted and the motive of committing the crime is benefit. Quick physical.

Some argue that the perpetrators of cybercrime are not of the same degree of seriousness and efficiency in the field of cybercrime, and on this basis they can be classified into two categories: the first are (used criminals), and these have experience in the field of electronic devices, even if it is a simple experience, and they are less dangerous. If they are compared to other criminals because they practice their talents in the information field for the sake of entertainment without appreciating the possible consequences that may occur as a result of their illegal actions[10] .

As for the second category, they are (programmer criminals), and these are more dangerous than other offenders because they have the capabilities and skills in the field of informatics from entering and breaking into the systems of electronic devices, as well as their ability to evade attempts to discover them by hindering the prosecutions of

10. Osama Ahmed Al-Naasa, Computer and Internet Crimes, 1st Edition, Dar Awael Publishing, Jordan, 2001, p. 82

11. Saad Hajj Bakri, the previous source, p. 210.

is devoted to indicating the place of inspection in information crimes, as follows:

First section

Definition of inspection in information crime

Criminal legislation dealt with inspection as a means of collecting evidence, but it was devoid of a text on its definition.[12] Therefore, jurisprudence took the task of setting a definition for inspection. There are those who defined it as "vision by eye of a place, person or thing to prove its condition and control everything necessary to reveal the truth." It was also defined as "a direct live observation and examination of a place, person or thing related to the crime to establish its condition and to disclose and preserve all things that may be useful in revealing the truth."[13]

Inspection is a procedure whereby the competent person moves to the place where the crime occurred to witness himself and collect the traces related to the crime and how it occurred, as well as collecting other things that are useful in detecting the crime.

The importance of the inspection appears in that it conveys to the competent authority an overall picture of the crime scene with all the details prejudice to the rights and fundamental freedoms of individuals.

We will discuss the means of collecting evidence, represented in inspection and control, each of which begins with a brief overview of the general rules related to it, and then we discuss those means in the field of their application in information crimes that represent a form of the new criminal intelligence, by dividing the research into two demands and as follows :

The first requirement

Inspection in information crime

Inspection is a means of collecting evidence at the stage of the preliminary investigation, and its importance appears in the context of traditional crimes after the crime, where there is an actual crime scene that contains actual material traces that the inspector reserves for examination and to indicate the extent of its validity in the evidence, but the matter is different in information crimes where It is rare for it to leave material traces, and the period between the occurrence of the information crime and its discovery may be long, which exposes the resulting effects to erasure, damage or tampering with.

In order to be aware of the subject of inspection in information crimes, we will deal with it in three branches. We dedicate the first section to the definition of inspection in information crimes. In the second section, we deal with the procedures of inspection in information crimes. The third section

12. Including the Iraqi Code of Criminal Procedure No. (23) of 1971 in Article (43) and the Egyptian Code of Criminal Procedure No. (150) of 1950 in Article thereof.
13 .Dr. Afifi Kamel Afifi, Computer Crimes, without a publisher, without a place of publication, p. 333

access to the system or site was made[15].

5- Proving the condition of the connections and cables connected to all components of the system so that the comparison and analysis process can be conducted when the matter is presented later to the judiciary.

6- Disconnecting the electricity from the inspection site to prevent the offender from taking any action that would affect the effects of the crime.

7- Not to transfer any information from the crime scene except after making sure that the outer perimeter of the electronic calculator site is free of any magnetic field that could cause the recorded data to be erased.

8- Reservation of what may be found in the trash of discarded or torn papers, tapes and CDs, examining them and removing fingerprints that may be related to the crime committed. By examining the trash in the location of the electronic calculator, a software theft crime was detected In Santa Clara, USA [16].

9- Recording inspection procedures to avoid losing evidence and preserving the crime scene.

15. Dr. Mamash Zahia and Ghanem Nassima, Criminal Evidence in Information Crimes, Master's Thesis submitted to the Faculty of Law - Abdul Rahman Mira University, 2012-2013, p. 12.
16. Ali Adnan El-Fil, Investigation Procedures, Evidence Collection and Initial Investigation of Information Crime, Modern University Office, 2012, pp. 33 and 34.

contained in this site, whether related to its location, its description from the inside, or a statement of the antiquities found therein[14].

second section

Inspection procedures in information crime

Due to the special nature of information crimes, it has become necessary to observe a set of procedures that the competent authority is obliged to follow before beginning to inspect them, which are as follows:

1- Identification of the electronic devices subject to inspection.

2- Conducting the inspection by investigators who have the scientific competence and technical experience in the information field.

3- Photographing electronic devices and other devices connected to it, with a focus on photographing the back parts of the calculator and its accessories, taking into account the recording of the time, date and place of taking each image.

4- Interest in knowing the method in which the system was set up and the electronic traces of the electronic records that are provided to information networks with the approval of the communication site and the type of device through which

14. Dr. Nadim Muhammad Hassan Al-Tarazi, Public Prosecution Authorities in Information Crimes, research published in Al-Andalus Magazine, Issue 13, Volume 15, 2017, p. 312.

crime scene as a place that can be inspected.

This difficulty consists of two things:

1- Few of the material effects that may be left behind from this type of crime.

2- The large numbers of people who may frequent the crime scene during the period between the commission of the crime and its detection, which is often relatively long, which can lead to changes or tampering with the material traces or the disappearance of some of them, which casts ambiguity on the evidence that can be obtained from conducting the inspection. [18]

The third requirement

Information Crimes Arrest

In order to understand the subject of seizure as one of the means of collecting evidence in information crimes, we will divide this requirement into two branches. In the first section, we deal with the definition of seizure in information crimes, and we devote the second section to determining the location of seizure in information crimes, as follows:

First section

Definition of seizure in information crime

Seizure can be defined in general as "seizing something related to a crime that has occurred and is useful in

18. Thanayan Nasser Al-Thunayan, Proof of Cybercrime, Master's Thesis submitted to the College of Graduate Studies - Naif University for Security Sciences, 2012, p. 57.

third section

Inspection place in information crime

Despite the importance that inspection occupies in the field of detecting the ambiguity of the information crime by proving the crime scene, it is not the same effective in controlling all the evidence of these crimes, due to the existence of a range of these crimes that are not suitable, by their nature, to be the object of inspection. Information crimes between what may be the subject of inspection and what cannot be considered as well as components of electronic devices, as follows:

First: Inspect the hardware components:

An example of these crimes is the assault on electronic calculator tapes, cables, its display screen, operating keys, disks and other components of a physical nature. By the competent authorities, and to keep what is considered material evidence that helps in committing the crime and attributing it to a specific person [17].

Second: Inspect the intangible components:

These crimes are characterized by the fact that they fall on the software of the electronic device, its data, and everything that is not material and tangible. In this type of crime, the difficulty appears in the validity of the

17. Dr. Afifi Kamel Ghafifi, previous source, pg. 336

the Code of Criminal Procedure No. (23) of 1971, we find that the legislator did not explicitly stipulate the seizure as one of the investigation procedures, but referred to it when he spoke about the provisions of the inspection from that text of Article (78). Which stipulated that "the search may not be done except in search of the things for which the search was conducted. If it appears during the search that there is in itself a crime or that is useful in revealing another crime, it may also be seized" and also Article (79) as it reads "to the investigator or a member of the judicial police." .... In the event of a flagrant premeditated felony or misdemeanor . In which persons or papers are seized .[21] .

This is in contrast to the behavior of the Egyptian legislator in the Code of Criminal Procedure No. (150) of 1950, which stipulated the seizure procedure in Chapter Four under the title (On movement, search and seizure of things related to crime) and articles (95-100) came to clarify its provisions.

As for the legislation related to information crimes, the Iraqi draft cybercrime law for the year 2011 stipulated the seizure procedure in Article (24/Third), which stipulates that "the investigative judge or investigator shall initiate the seizure procedures..." and Article (26) stipulated that First - The competent judge may: Seize the computer hardware or part of it or the medium in revealing the truth about it and its perpetrators, whether this thing is real estate or movable, and the seizure may be returned to people, which is what is termed as arrest .[19]

Seizure is one of the means of collecting evidence, as is the case with the search, which aims to reach evidence that is useful in detecting the crime, although in some cases it is considered a result of the search, but it can be taken as an independent measure without resorting to inspection, as the detection of the scene of the accident may lead to it. It can also be the result of things presented by witnesses or accused persons, so the control has its rules and conditions that the competent authority is committed to. It is only permissible in things that help to reveal the truth, such as weapons and tools used in committing the crime and the clothes of the offender or the victim if found on them. The effects of the crime of blood and others, and the most important thing that distinguishes the seizure from the search is that the seizure does not infringe on confidentiality, as it affects only financial rights such as the right of ownership and possession. Inspection whose purpose is control is the one that affects the sanctity of the secret[20] 20.

As for the opinion of the Iraqi legislator regarding the seizure procedure, through the provisions of

21. Articles (83) and (84/b) of the Code of Criminal Procedure No. (23) of 1971.

19.Bakky Fatima al-Zahra, p. 79.
20. Dr. Saleh Abdul-Zahra Al-Hassoun, Provisions of Inspection and its Effects in Iraqi Law, 1st Edition, 1979, p. 70

second section

The place of arrest in the information crime

It is necessary to distinguish in the place of arrest in the information crimes whether this place consists of the physical components of the electronic devices or the intangible or intangible components of these devices:

First: Adjust the hardware components:

The basic principle with regard to tuning is that it refers to physical objects that can be placed by hand. Therefore, tuning the physical components of electronic devices and their accessories does not pose any problem as they are physical objects, and therefore it is permissible to set wires and switches for the input unit, modem, memory unit, and control unit, and including the outputs in the picture Paper outputs or media and physical storage containers such as magnetic disks and tapes, where the tool or medium in which the storage takes place is set.

Second: Adjusting the intangible components:

The subject of controlling the intangible components of electronic devices has raised a wide disagreement among jurists, as an opinion of them went to say that intangible entities are not suitable for being a subject of control, and the reason for this is that the texts of the procedural laws require the tangible physical nature of these which the data was stored and transferred to the investigation authority for analysis and study, and he may copy it without transferring the system and remove the data that prevents entry to the computer without causing damage to the system or compromising the integrity of the data and programs stored in it.

This is what the Palestinian legislator followed in the Palestinian Cybercrime Law No. 16 of 2017, however, it was more detailed in its statement of the provisions of control in cybercrime than it was treated in the Iraqi draft law on cybercrime, where Article (34) of the Palestinian Cybercrime Law A treatment for everything related to the seizure procedure, starting with the authority competent to carry it out, indicating the place of seizure and the means of seizing the items subject to seizure until the necessity of writing a record of what was seized.[22]

As for Article (6) of the Egyptian Information Technology Crimes Law of 2018, it stipulates the seizure procedure when it stipulates: "1- Seizure, withdraw, collect or retain data, information or information systems and track them in any place, system, program, electronic support, or A computer in which it is located, and its digital evidence is delivered to the authority issuing the order, provided that this does not affect the continuity of the systems and the provision of the service if necessary.

22. Article (34) of the Palestinian Cybercrime Law No. (16) of 2017.

controlled, to include the processed data in its intangible form[24]

Conclusion

At the end of this study, it was necessary for us to present the most important results that we reached, as well as to highlight the most important recommendations and suggestions that deserve to be put forward.

Results :

1- Through the study, we concluded that the legal thought did not settle on a specific term for information crime, there are those who called it the term (information fraud) and others used the term (information embezzlement), and there are those who called it, which we agreed with (information crime).

2- The research showed that the information crime has some characteristics that distinguish it from traditional crimes in that it is a crime that crosses international borders, and it is less violent than the traditional crime as it does not require physical effort from the offender, as it depends on thinking, mental effort and sufficient knowledge of information technology.

3- The study proved that the information criminal has features that are often not available to the traditional criminal, as this criminal is characterized by advanced skills and sufficient knowledge of ways to use entities in order to be suitable for being a subject of control .[23]

A second trend was that the concept of control could be extended to include electronic intangible components, and this trend finds its legislative embodiment in the laws of some countries such as Canada, Greece and the United States of America, which stipulated that investigation authorities be given the ability to do anything that is necessary to collect and protect evidence, including intangible components. And if it is not imagined that it be set as intangible things, it is possible to set it if it has a physical entity, such as setting the solid piece as a storage tool for evidence, information and data to be set on paper or recorded on tapes or discs or copied into files, as in this case it turns The intangible components into things that are visible and readable and acquire a physical entity by which they can be controlled and transferred from one place to another, and the same saying applies to electronic messages.

There is a third and final trend that its proponents see is that there is no point in applying the texts of the current procedures related to control to the electronically processed data in its abstract form from its physical support. Rather, the legislator must intervene to expand the range of things that can be

24. Dr. Miftah Bu Bakr Al-Matradi, Cybercrime and Overcoming Its Challenges, Research Presented to the Third Conference of Chiefs of Supreme Courts in the Arab Countries, 2012, pg. 46

23. Youssef Khalil Youssef, Electronic Crimes in Palestinian Legislation, a master's thesis submitted to the College of Sharia and Law - The Islamic University - Gaza, 2013, p. 124.

2- We recommend the legislative authority in Iraq to expedite the approval of the draft information crimes law for the year 2011 because of the provisions it contains regarding information crimes. Without committing information crimes against them.

The references

Legal books:

1. Osama Ahmad Al-Manasah, Computer and Internet Crimes, 1st Edition, Wael Publishing House, Jordan, 2001.

2. Osama Ahmed Al-Manasah, Information Technology Crimes, 1st Edition, Wael Publishing House, Jordan, Amman, 2001.

3. Jamil Abdel-Baqi Al-Saghir, Criminal Law and Modern Technology, 1st Edition, Dar Al-Nahda Al-Arabiya, Cairo, 1992.

4. Rami Metwally Al-Qadi, Combating Information Crimes, Dar Al-Nahda Al-Arabiya, Cairo, 2011.

5. Salih Abdul-Zahra Al-Hassoun, Provisions of Inspection and its Effects in Iraqi Law, 1st Edition, 1979.

6. Afifi Kamel Afifi, Computer Crimes, without a publisher, without a place of publication.

10. Ali Adnan El-Fil, Investigation Procedures, Evidence Collection and Initial Investigation of Information Crime, Modern University Office, 2012.

information systems, which is what is required by the nature of committing information crimes.

4- Extrapolating the texts of the Iraqi draft law on information crimes for the year 2011 showed us that it referred everything that was not mentioned in this law to the Iraqi Code of Criminal Procedure No. (23) of 1971, and this is what we saw in the means of collecting evidence in information crimes from a preview and adjust.

5- The study revealed to us the insufficiency of the means of collecting evidence, represented in the inspection and control contained in the traditional texts in the face of information crimes, because the nature of the place in these crimes differs from what is found in traditional crimes, as the information crime is often committed on a place that enjoys its moral and immaterial nature. From a special treatment of these crimes in special legislation to find a kind of integration between these legislation and the traditional texts.

Recommendations:

1- We suggest to our Iraqi legislator organizing a mechanism for cooperation between the courts specialized in information crimes and between companies or institutions with jurisdiction in the field of electronic devices and social media such as (Viber) and (WhatsApp) that these companies provide the courts with information that helps the courts in the investigation about these crimes.

Information in Combating Crime, The Arab Journal for Security Studies and Training, p. 6, p. 11, Riyadh, 1990.

3. Muftah Bu Bakr Al-Matradi, Cybercrime and Overcoming Its Challenges, Research Presented to the Third Conference of Chiefs of Supreme Courts in the Arab Countries, 2012.

4. Nadim Muhammad Hassan Al-Tarazi, Public Prosecution Authorities in Information Crimes, research published in Al-Andalus Magazine, Issue 13, Volume 15, 2017.

Laws:

1. Egyptian Criminal Procedures Law No. 150 of 1950.

2. The Iraqi Code of Criminal Procedure in force No. 23 of 1971.

3. Palestinian Cybercrime Law No. 16 of 2017.

4. The Iraqi draft law on information crimes for the year 2011.

5. The Egyptian Information Technology Crimes Law of 2018.

6. American Computer Crimes Law No. (1213) for the year 1986.

7. Saudi Cybercrime Combating Law No. (17) for the year 1428.

The Agreements:

European Convention on Information Crimes. Budapest for the year 2001.

12 . Muhammad Ali El-Dian, Electronic Crimes, New University House, Alexandria, 2011.

13. Nahla Abdel Qader Al Momani, Information Crimes, 1st Edition, House of Culture, 2008.

14- Huda Hamid Qashkoush, Computer Crimes in Comparative Legislation, Dar Al-Nahda Al-Arabiya, Cairo, 1992.

Theses

1. Thanayan Nasser Al-Thunayan, Proof of Cybercrime, Master's Thesis submitted to the College of Graduate Studies - Naif University for Security Sciences, 2012.

2. MamashZahia and GhanemNasima, Criminal Evidence in Information Crimes, Master's Thesis submitted to the Faculty of Law - Abdul Rahman Mira University, 2012-2013.

3. Youssef Khalil Youssef, Cybercrime in Palestinian Legislation, a master's thesis submitted to the College of Sharia and Law - Islamic University - Gaza, 2013.

Researchpapers :

1. Khalil Youssef Jundi, The Legislative Confrontation of Information Crime at the International and National Levels, Research published in the Journal of the College of Law for Legal and Political Sciences, No. 26, Volume 7, 2018.

2. Saad Al-Hajj Bakri, Communication Networks and the Employment of