How to Cite:
Alnakeep, H. T. (2022). Internet crimes to legal regulation. *International Journal of Health Sciences, 6*(S7), 6833-6853. https://doi.org/10.53730/ijhs.v6nS7.13683

Internet crimes to legal regulation

Huda Talib Alnakeep
Dijlah University Collage
Email: Huda.talib@duc.edu.iq

***Abstract*---**With the spread of modern means of technology among individuals in societies and the widespread use of them and the expansion of dealing through them, every individual in society can communicate without any barriers or geography, with the availability of the ability to transmit and receive information and technologies, to obtain data and programs with all ease, and with the many advantages and benefits that accompanied the emergence of this new and advanced technology of science and knowledge, but this was accompanied by the emergence of many problems and negatives that appeared in the form of a crime committed by some users of technology, which is characterized by its danger and ease of committing and the dilemma of crossing the borders, which can be called cyber. It was necessary to confront these crimes through multiple means, including criminal legal protection, which is considered the most important means of society in maintaining its security and protecting its interests. However, with the modernity of these crimes and the modernity of the legislation regulating criminal protection in all fields and fields, there is still a shortcoming in delineating the limits of this protection from the penal aspect, which requires attention and expediting the provision of sound legal frameworks and clear procedural references to combat this dangerous type of crime

***Keywords*---**crimes, Legal, technology

Introduction

In our present age, which is witnessing a huge information revolution, where science and discoveries race to appear every morning, announcing strong and sharp competition in this field. In the beginning, the Internet appeared with its limited uses, but it expanded and spread rapidly in record time, and its users became of all age groups and at different levels of education, and thus opened closed doors and sounded the alarm, as this network remained unguarded and without restrictions or limits to deter bad deeds that always come from humans, this is the reason and as an inevitable result of any new technical progress that led to the emergence of the so-called internet crime, which came to alert the

communities to the greatness of their danger, as it expanded its scope and its professionalisms appeared to steal, loot and sabotage, which led the societies to recognize the necessity of taking a strict stance towards them. And the quick resort to finding solutions, the essence of which was to know the nature and purpose of internet crime, and knowing its forms, how to prevent it, and its owners. From this emerged the importance of knowing internet crime and the need to educate and educate about the nature, danger and objectives of these crimes.

The purpose of the Study

The topic of internet crimes is gaining increasing importance due to the increasing exploitation of modern means of communication by perpetrators of crimes to facilitate the commission of their crimes, and the fact that Internet crime threatens the national security of countries and affects the interests and privacy of individuals and threatens the information system of companies, so the importance of this research lies by identifying some images of Internet crimes for the purpose filling the gaps in the Iraqi legislation regarding these crimes and to reduce Internet crimes

The Problem of the Study

The technical development that occurred in the last decade was accompanied by a great development in the methods of committing Internet crimes that take place via computers or smartphones, which requires the legislator to legislate and update laws constantly to confront the legislative and penal vacuum for this type of crime and to confront the malicious methods and programs that arise every day.

The aim of the Study

This research aims to define the nature of Internet crimes, their legal nature and their moral and material pillars by reviewing some of the illegal images used by terrorist organizations and drug dealers and their use in pornographic and immoral crimes and clarifying the position of the Iraqi legislator regarding Internet crimes and the position of legislation the comparison also, and this research also aims to put our findings and recommendations in this research in the hands of the Iraqi legislator to reach an integrated legislation aimed at confronting these crimes and limiting them to preserve the security and privacy of individuals and filling the gaps in the face of the rapid development of these crimes.

Research Plan

Chapter One

The concept of internet crime and its elements

Internet crime requires special and great knowledge of computer technologies and information systems to commit it, investigate it, prosecute its perpetrator or

prevent it. For this crime to take place, its three pillars must be fulfilled, which are the material pillar, the moral pillar, and the legal pillar.

The First Requirement

Internet crime concept

It is very illegal behaviour that is carried out using electronic devices, resulting in the criminal obtaining material or moral benefits with the victim bearing a corresponding loss Often the goal of these crimes is hacking to steal or destroy information. (1(

The modernity that characterizes internet crime and the different legal and cultural systems between countries has led to a difference in the concept of cybercrime. According to the European Commission, the term cybercrime includes all the traditional manifestations of crime such as fraud and falsification of information, publishing electronic materials with immoral content or a case for sectarian commotion, and according to the Department of Justice in the United States of America, which defined crime via the Internet as any crime whose perpetrator has technical knowledge of technology and according to the Economic Cooperation Organization, a crime committed via the Internet is any illegal, immoral or unauthorized behaviour related to the automated processing and transmission of data. The term Internet Crimes was launched at the Internet Crimes Conference held in Australia in 1998 (

Despite the relative modernity of internet crime, it has received attention from some researchers, as many different studies have been conducted to try to understand this phenomenon and then control it, including a study conducted by the Business Software Alliance in the Middle East, which showed that there is a discrepancy between the countries of the region in the Middle East, the amount of computer crime losses ranged between (30,000,000) three million US dollars in the Kingdom of Saudi Arabia and the United Arab Emirates, and also (1,400,000) one million and four hundred thousand US dollars in Lebanon (3)

And if it is very difficult to follow up and detect Internet crimes, as these crimes do not leave a trace, and there is no lost money or jewellery, what are the numbers that change in the records? And most computer crimes were discovered by chance and after a long time from their commission, and the crimes that were not discovered are much more than those revealed by the cover-up (4).

The Second Requirement

Elements of Internet crime

Internet crimes, like other crimes, require the availability of the agreed-upon pillars for the necessity of establishing them and for them to exist on the ground. Therefore, the physical, moral and legal pillars must be present

Section one

Material Pillar

We know that the material element of the crime in general is criminal behaviour by committing an act criminalized by law or refraining from doing something ordered by law (5.(

Therefore, it is the external material behaviour that the law stipulates criminalizing, that is, everything that enters the entity of the crime and has a material nature, so the senses touch it, and it is necessary for its establishment, as the law does not know crimes without a material element, and that is why some called it the materialities of the crime, which results in it is not considered one of the before the material pillar is the thoughts, desires, and aspirations that come to mind as long as they do not take their way to the external space with a tangible appearance due to the absence of the material pillar in them (6). And the material element in Internet crimes, like other crimes, consists of three elements: criminal behaviour, harmful result and causation relation.

1.Criminal behavior

Committing a crime via the Internet requires the offender to practice a technical activity, that is, providing a necessary level of awareness of the use of the Internet and the computer. There are many examples of Internet crimes, and they are many, including a person who publishes explicit sexual pictures of adults and children and modern technology is used in these pictures by placing the heads of well-known people such as artists on the bodies of other naked people, a crime that falls under the section on crimes against public morals (7.(

may occur via the Internet, as the offender defames his colleagues, his superiors at work, or the political leaders of countries, and their purpose may be to cure or love to appear and shed light on him, and this is what happened in 2002, where one of the citizens directed several insults and to the King of Jordan via the Internet (8 .(

Among the criminal behaviour in which espionage crimes are realized through the Internet is that the perpetrator inserts a spying file into the victim this file is called a Trojan horse, and the spying file is inserted into the victim's device through three methods, either through chat programs, where the hacker sends a file to the victim and assures him that it contains exciting toys or other temptations, so the victim is deceived and receives the file. The second method is via e-mail, where the hacker sends a message to the victim and he opens it and finds that it contains attached files that carry a hacking program. The third method is a visit to unknown sites that tempt him to download some free programs and files, including the spyware file (9)

The behaviour may be achieved in the intentional, illegal entry into data processing systems related to electronic commerce, obstructing or distorting the operation of data processing systems related to electronic commerce, or tampering with data systems (10)

we note that the criminal behaviour in Internet crimes is not limited to the same behaviour that is achieved by other crimes hence, any criminal behaviour that is commensurate with the nature of the right that is being attacked; an Internet crime can be realized.

2.Harmful result

The harmful result or the criminal result of Internet crimes is the change that takes place in the outside world as an effect of the criminal behaviour, and it achieves aggression that obtains an interest or a right that the legislator assesses as worthy of criminal protection Which means that the harmful result has two connotations, one of which is material, which is the change resulting from criminal behaviour in the outside world, and the other is legal, which is the aggression that obtains its interest or a right protected by law.

3. Causal relationship:

For an Internet crime to occur, there must be a physical link between the material behaviour and the achieved criminal result. For example, for the crime of violating the right to privacy or espionage via the Internet, there should be access to the Internet using a working computer and penetration of the various servers in its path and then infringement on the privacy of a site (11).

An important note is that cybercrime spreads the idea of probabilistic outcomes result of the original crime, and this is due to the nature of the technical activity in these crimes, so whoever intends piracy in his behaviour and results in the spread of viruses, is considered a possible result of that work (21).

Section Two

The Moral Pillar

It indicated that Internet crimes need high technology to be committed, and therefore these crimes are of the type of intentional crimes, that the perpetrator of these crimes has planned and plotted to commit them, whether to obtain information or to penetrate another computer network. For example, whoever insults, slanders, steals, espionage or damages via the Internet, undoubtedly, has the knowledge and the will for what he is doing, and they are the two elements of criminal intent required for the moral element of the crime to be established (13).

However, some believe that Internet crimes can achieve intrusive intent, such as if a person sent a virus via e-mail to one of the individuals to take revenge on him, causing the virus to invade every computer connected to this server. Here, the person's intention has exceeded what he was aiming to achieve, as they see that Internet crimes may occur unintentionally as a result of the error, such as the destruction of the institution's devices as a result of excessive use by the responsible employee who uses the computer belonging to it with operations for his account, relying on his skills in avoiding viruses (14).

Section Three

Legal Pillar

As for the legal pillar, it is the illegal character of the behaviour, and that is by applying the behaviour, whether it was an act or an omission, to a text in the law that criminalizes it. In Iraq, like most Arab countries, special laws for Internet crimes have not been enacted, and therefore the matter of criminalizing them is left to the general rules of the penal code and the complementary laws to it, while we note in Egypt that it was stipulated in the Communications Law of 2003 as well as the Intellectual Protection Law of 2002 (15).

Chapter Two

Internet crime images

In this chapter, we will deal with the most important of these images (the use of the Internet by terrorist organizations, and other crimes committed via the Internet).

The First Requirement

Using the Internet by Terrorist Organizations

And it has become to include more dangerous activities represented, as one researcher points out, specialized in the daily use of the Internet by terrorist organizations to organize and coordinate their scattered and spread operations around the world. The active terrorist presence on the Internet is scattered, diverse, and highly elusive. If a terrorist website appears today, its electronic pattern quickly changes and then disappears to reappear in a new form and a new email address after a short period. The websites of these organizations not only address their supporters and financiers but also direct Their messages are also to the media and the public for the gatherings that terrorize and terrorize them, to launch psychological campaigns against the targeted countries. They show horrific films of the hostages and prisoners during their execution, at the same time the terrorists claim that they have noble causes, and they complain of mistreatment by others.

Examples of some Arab websites that were created and designed by some terrorist organizations are as follows (16) :

Al-Nida website: It is the official website of Al-Qaeda after the events of September 11, 2001. Through it, Al-Qaeda's media statements are issued.

Dharwad Walsingham: It is a periodical electronic newspaper for the media department of Al-Qaeda.

Sawt Al-Jihad: It is a semi-popular magazine, issued by the so-called Al-Qaeda Organization in the Arabian Peninsula, and it is issued in two formats: (word),

and (pdf). It includes a set of statements and dialogues with the organization's leaders and theorists.

Al-Battar: It is a specialized electronic military magazine. Issued by Al-Qaeda, it specializes in military and field information and recruitment.

Among the most basic elements of using the Internet for terrorist purposes are:

Information Prospecting: The Internet itself is a huge electronic library, and it is full of sensitive information that terrorists seek to obtain, such as the locations of nuclear facilities and information on ways to combat terrorism. Thus, 80% of their information stock is based mainly on websites available to everyone, without violating any laws or network protocols.

Communications: The Internet has helped the scattered terrorist organizations to communicate and coordinate with each other, due to the low costs of communication using the Internet, compared to other means, and it is also characterized by an abundance of information that can be exchanged, and the absence of a visible leader of the terrorist group has become an essential feature of the modern terrorist organization, different from the old hierarchical pattern of terrorist groups, and all this because of the ease of communication and coordination across the global network.

Mobilization and Recruitment of New Terrorists: Bringing new elements into terrorist organizations maintains their survival and continuity, and they take advantage of the sympathy of others through electronic chat rooms, We know that the entertainment of young people and teenagers is sitting for long hours in Internet cafes to gossip with all kinds of people in different parts of the world.

Giving instructions and Electronic indoctrination: The Internet is filled with a huge number of sites that contain brochures and instructions explaining the methods of making bombs, and lethal chemical weapons, When Google search engines were used in 2005 to search for sites with the words "terrorist" and "handbook" in their topics, the search results came to nearly 8,000 sites.

Planning and Coordination: The Internet is a very important means of communication for terrorist organizations, as it allows them the freedom to coordinate closely to launch specific terrorist attacks, and Weiman adds that prominent members of Al-Qaeda relied extensively on the Internet in planning the September 11 attacks, and terrorists use email and chat rooms, to manage terrorist attacks and coordinate the actions and tasks of each terrorist element.

Obtaining funding: Terrorists use demographic data selected from the personal information that users enter on the network through inquiries and surveys on websites, to identify people with compassionate hearts, and then they are begged to pay financial donations to legal persons, who represent a front for these terrorists. This is cunningly done by e-mail, in which the donor does not suspect that he is helping one of the terrorist organizations.

Some attribute the causes of electronic terrorism to a group of political, economic, social, intellectual and psychological reasons, and they can be described as general reasons that are not difficult for anyone knowing it, but there are a set of reasons, which are known as the special or main reasons behind the spread of the phenomenon of electronic terrorism, and they can be summarized as follows (17):

1- The weakness of the structure of the information networks, their lack of privacy and their vulnerability to penetration

The information networks are originally designed openly without restrictions or security barriers to expand and facilitate the entry of users. It contains electronic systems and information networks that terrorist organizations can exploit to infiltrate infrastructure and carry out terrorist sabotage operations.

2. Absence of geographical borders and low level of risk

The absence of spatial boundaries in the information network, in addition to the lack of clarity of the digital identity of the user settled in his open environment, is a suitable opportunity for terrorists, as the computer professional can present himself with the identity and the capacity he wishes to hide with a fictitious personality.

3- Ease of use and low cost

Social media and all electronic means of communication have become cheap and available in all countries of the world, other than in the eighties of the last century. The global feature of information networks is that they are an easy-to-use and low-cost method, which created an opportunity for terrorists to reach their illegal targets and carry out their electronic attacks.

4- Regulatory and legal vacuum

That is the lack of regulatory and legal frameworks for information crimes and cyber terrorism. And if there are laws, the criminal can start from a country where there are no strict laws, and here the problem of conflict of laws and the law and its application will arise.

5- The difficulty of detecting and proving cybercrime

Technology can only determine the identity of the perpetrator of the electronic crime through certain devices owned by some security institutions, but individuals cannot determine that.

Cybercrime has become a whisper that preoccupies countries that have become vulnerable to attacks by terrorists and extremist groups via the Internet and new media of all kinds. It became clear that these groups practice their terrorist activities from anywhere in the world and at any moment. These dangers are increasing day by day because modern technology alone is unable to protect

people from electronic terrorist operations, which in turn have caused great damage to individuals, institutions and countries.

Accordingly, it cannot be said that there are completely guaranteed ways to protect the information system from penetration to this day. However, most countries and institutions sought to adopt a set of electronic procedures, which were in the form of a set of devices, systems and programs integrated according to a pre-established program to address any intrusion into information systems to technically protect them from terrorist attacks. As many countries have sought to take the necessary measures and measures to address terrorism and electronic mail.

However, these efforts are limited and still need more studies, research, legislation and regulation due to the seriousness of this phenomenon. Among these procedures that countries must take to combat electronic terrorism are the following(18):-

1. Monitoring the activities of terrorist groups on social networks and analyzing their content, objectives and strategies adopted in them.

2. The participation of civil society and its institutions in cooperating to report on the site related to terrorism and terrorists.

3. Work to spread the preventive culture and raise society's awareness of the dangers of terrorism in general and electronic terrorism in particular, and to confront it by rejecting hatred, violence and the culture of exclusion, spreading the culture of tolerance and dialogue with the other, and respecting different religions and cultures.

4. Enact special laws and legislation that fill all gaps that discover the crime of electronic terrorism or ways to investigate it, and laws related to how to discover and preserve electronic evidence.

5. Creating an international legal system under the umbrella of the United Nations entrusted with documenting and unifying the efforts of countries to combat and confront electronic terrorism.

6. Concluding international agreements regarding cyber terrorism crimes and organizing all procedures related to the exchange of information and evidence that would activate agreements to extradite perpetrators of cyber terrorism crimes.

7. Strengthening international and regional cooperation through the monitoring of electronic criminal acts on its territory by each country against a country or other parties outside these territories with the help of international organizations and authorities specialized in combating electronic terrorism.

8. Organizing scientific conferences and introductory symposiums in universities and specialized research centres in various countries of the world that include experts and researchers from various fields to study the problem and develop appropriate solutions to it.

In light of the foregoing, it becomes clear to us the extent to which this type of terrorism is linked to scientific and technological progress, which is in a state of continuous and non-stop progress as long as the human mind works. Accordingly, there is a direct relationship between the two; The more technical and informational progress occurs, the greater the risk of electronic terrorism.

The Second Requirement

Other crimes committed on the Internet

Some types of crimes committed via social networking sites can be mentioned as follows:

First: impersonation:

This is considered the new millennium crime, as some specialists in information security called it, due to the rapid spread of its commission, especially in commercial circles, and this crime is represented in the use of another personal identity illegally and aims either to benefit from its place, that identity, that is, the identity of the victim, or to conceal the identity of the criminal to facilitate his commission Other crimes (19).

Second: immoral and sexual pornography crimes:

If the Internet has a positive aspect, it has a negative and dangerous aspect, and one of these aspects is the presence of websites on the Internet that offer and incite sex, whether with adults or with children, these sites publish more specialized sexual images, including those specializing in video films, some of them specialize in images, and many of them specialize in chat programs. These sites are very popular in visiting and browsing their content.

It turned out that there was a report published by CNN on its websites on March 15, 2002, in which it was stated that porn sites are easy to access and that the rate of flow to visit these sites during working hours, which starts from nine in the morning until five in the afternoon, is about 70% of the total flow rate to visit these sites.

Arab porn sites, not foreign ones, were counted in some sites on the Internet, and it was found that they reach 71 sites, and the number of most of them have reached 8683 members, and the number is increasing (20).

Does a question arise about the effect of pornography on the deterioration of values and the spread of crime?

Psychologist Edward Donner of Duskusson University in America has found for years that those who engage in prostitution and pornography often affect their behaviour from an increase in violence and indifference to the misfortunes of others and acceptance of rape crimes, and many researchers have found that such porn is inherited.

Third: Drug trafficking using the Internet:

Fears of using the Internet are not limited to the use of the Internet to commit a crime, but some sites contribute to the deviation of young people, especially adolescents, through the creation of websites with the intention of trafficking in drugs or psychotropic substances, promoting them, using them, or facilitating dealing with them, or contracting, dealing or negotiating to conclude transactions related to trafficking in any form.

Chapter Three

Legislative position on Internet crimes

One of the most dangerous and most prominent crimes in our time is the crimes that are carried out via the Internet and the computer via e-mail and various social media, and their danger to national security and society. Most countries of the world have enacted laws criminalizing this situation. The Iraqi legislator and the position of comparative legislation in the countries of the world in two separate requirements.

The First Requirement

The position of the Iraqi legislator on Internet crimes

Article (1/12) of the Iraqi Information Crimes Project for the year 2011 defined information as: “data, text, images, shapes, sounds, symbols, databases, computer programs and the like that are created, stored, processed or sent by electronic means” (21).

As for the position of the Iraqi legislator regarding the definition of Internet crimes, it issued a project information crime law for the year 2011, which was issued based on the approval of the House of Representatives and the approval of the President of the Republic. In the context of the definition of information crime, the legislator did not put in the aforementioned project a specific definition of information crime, only enumerating the acts that constitute information crimes. Thus, each of these crimes can be considered a definition of information crime. Through extrapolating the texts of the information crime project, it becomes clear that information crime is the use of a computer to commit one of the following crimes (22):

1- Crimes related to the country's independence, security and unity (political - security).

2-Crimes related to financial disclosure such as misuse of bank cards and magnetic cards and storming banks and financial markets - signing bonds - forging financial or personal bonds - tampering and manipulating any data and statements related to financial shares.

3- Crimes related to persons, crimes of defamation, insults and slander, impersonation and talking about a specific personality - crimes related to

personalities and data related to private life, including crimes of assault on confidential data - fraud and deception - deception and luring - harassment and stalking - blackmail.

4- Trafficking crimes: human trafficking - drug trafficking - money laundering - sexual crimes and immoral practices - pornographic websites and mailing lists.

5- Sole proprietorship crimes: copying or publishing through the information network, intellectual works - press photo-processing crimes.

6- Other crimes: Internet auctions crimes - piracy crimes - forgery crimes and electronic document industry - Internet gambling - computer virus industry hacking crimes.

Iraq has joined the complex of development and submitted the draft cybercrime law for the year 2011 (23), and we hope that this project will see the light to impose legal protection on the Internet and punish the perpetrators of cybercrime, as well as submit the draft electronic signature and electronic transactions law for the year 2011 (24).

But on the other hand, we find that the Iraqi Information Crimes Project has permitted tracking information to computer systems and other suspicious networks. Article (26/first/c) stipulates that:“ Access to computers and networks or any part of them and the data stored in them and to any medium or means in which computer data inside Iraq may be stored, and the data is intercepted, monitored and controlled by a reasoned decision, for a specific period and purpose.” From the extrapolation of the aforementioned text, it becomes clear to us that the project has implicitly authorized the inspection of the physical and logical components of the computer, because it stipulates: “Access to computers and networks and the data stored in them .”

But at the same time, it stipulated guarantees for the inspection, as it stipulated several conditions, namely (25):

a . That the search was issued by a reasoned judicial order and that it was issued by the specialized judge.

b. Determining the duration and purpose of the search warrant.

c. Inform the authorities that own the systems under the inspection of the inspection procedure.

d. Determining the scope of the inspection about the conduct under investigation without violating or prejudicing the rights of others.

But we need to explicitly state the permissibility or possibility of inspecting the logical components of the computer, so we see the need for the legislator to explicitly state that the logical components may be inspected, because of the danger involved in the inspection and the rules that must be observed.

In Iraq, despite the issuance of the draft computer crime law for the year 2011 AD, we do not find in it a text similar to what was stated in the comparative laws to deal with inspections extended outside the borders of the state and refer to the project to what is not stipulated in the Code of Criminal Procedure in Article (30/second).) of the draft law on information crimes and concerning the Code of Criminal Procedure No. (23) of 1971 AD, we find that the first chapter of Chapter Seven of it has been devoted to the subject of judicial delegation in Articles (353-356), Where we find that Article (353) of the Code of Criminal Procedure expressly stipulates that a foreign country wishing to take an investigation procedure in a crime must be sent by the Iraqi authorities to send a request through diplomatic means to the Ministry of Justice (26), and in return for the Iraqi judicial authorities in the event of their request Delegating the judicial authorities in another country to take a specific action to send their request through diplomatic means to the judicial authorities in that country, as stipulated in Article (355) of the Iraqi Code of Criminal Procedure.

computers located in public places, such as the personal computers that a person carries outside his home, we see that the inspection of their systems is not permissible except in the cases in which the law permits the inspection of the person, given that the inspection of a person is all of himself and all that is in his possession at the time of performing the inspection, and whether it is owned by him or others.

In the case where the computer whose systems are to be inspected is inside a person's home, the restrictions stipulated by law about inspecting the residence of the accused or searching the house of a person other than the accused shall apply to it (27).

Wiretapping and other forms of electronic surveillance, although controversial, are permitted under certain circumstances in almost all countries. The permanent Iraqi constitution of 2005 AD guarantees freedom of communications and electronic postal, telegraphic and telephone communications and prohibits monitoring, wiretapping or disclosure except for legal and security necessity and by a judicial decision. The Iraqi constitution permitted wiretapping and electronic monitoring, but within certain limits, which is a legal necessity and the issuance of a judicial decision to that effect. Also, Article (26/first/c) of the project law on information crimes allowed data interception, monitoring and control by a reasoned decision, for a specific period and purpose, and the French law issued on 7/10/1991 Allows interception of telecommunications, including information exchange networks(28).

As for the position of the Iraqi legislator on the issue of testimony in cybercrime, we note that the information crimes project is devoid of any regulation for this issue, except that Article (30/second) refers to what is not stipulated in the project to the Code of Criminal Procedure No. (23) of 1971 M. Accordingly, about regulating the issue of testimony in cybercrime, we refer to the general rules of testimony in the Code of Criminal Procedure, but we see the necessity of regulating testimony in cybercrime because it is different from testifying in traditional crimes. After all, the witness, for example in the traditional crime, is one of the people who saw or he heard or witnessed something related to the

committed crime and he may be a relative of the offender. As for the witness in Internet crimes, he is one of the people mentioned (computer operator, maintenance engineer, programmer or analyst), so we see the necessity of expressly stipulating it in the project law on information crimes, Nevertheless, we believe that the information witness is obligated to give testimony if he possesses essential information necessary to obtain evidence, but in all cases, the witness must not be compelled to make him give the information, or else the testimony was flawed, and the result was the invalidity of the testimony. In this case, compulsion can be imagined, forcing the witness to give secret passwords.

Among the forms of activity in the crime of tampering with the system or data is the use of various virus programs that erase data or distort its content, as well as remote interference in the system and destruction of existing files. The Iraqi legislator stipulated in the project information crimes law criminalizing these acts within the scope of Internet crimes, where Article (7/Third) stipulates that: "He shall be punished by temporary imprisonment and a fine of no less than (10,000,000) ten million dinars and not more than (30,000, 000) Thirty million dinars for each of tampering, manipulation, images, altering or fabricating any data, statements or programs related to financial shares, documents, or currency rates traded inside Iraq or that are used by parties inside Iraq in the activities of trading financial shares, documents or currencies that take place outside Iraq on behalf of others." Article (15/second) of the aforementioned draft stipulates that: "The penalty shall be imprisonment for a period of no less than (four years) and a fine of no less than (15,000,000) fifteen million dinars and not more than (25,000,000) twenty-five million. If the act stipulated in Clause (First) of this Article results in the deletion, destruction, alteration, defect, disruption or re-publishing of data or information belonging to third parties without right.

Article (14/Third) of the Iraqi project of information crime law for the year 2011 stipulates that: "A penalty of imprisonment not exceeding (3) three months and a fine of no less than (2,000,000) two million dinars and not more than (5,000,000) five million Dinars for each of C - deliberately enters without permission (29) a website or information system, or communicates with a computer system or part of it, d - uses or causes without authorization the use of a computer belonging to others, directly or indirectly. Article (15/first) stipulates: "A penalty of imprisonment and a fine of no less than (10,000,000) ten million dinars and not more than (15,000,000) fifteen million dinars shall be imposed on whoever: A- Willfully exceeds the scope of the authorized declaration or obstructs any information during their exchanges" (30).

The Second Requirement

The position of comparative legislation on Internet crimes

Confronting cyber crime has met global attention, as various conferences and seminars have been held, and laws and legislations have been issued through them criminalizing those who commit these crimes. Sweden is the first country to enact legislation on computer and Internet crimes, as the Swedish Data Law was issued in 1973, which treats cases of computer fraud, in addition to including

general paragraphs that include crimes of illegal access to computer data, forgery, transfer or illegal access to it. The United States of America after Sweden enacted a law on the protection of computer systems in the period from 1976-1985, and in 1985 the National Institute of Justice identified five main types of information crimes, which are internal computer crimes, crimes of illegal remote use, and crimes of computer manipulation, support for criminal transactions, theft of ready-made programs and computer hardware. In 1986, a legislative law was issued in which all the necessary terms to apply the law to information crimes were also established, and the necessary constitutional requirements for application were established, And as a consequence, crimes arose, including the Texas Computer Crime Law. In 2000, the US Department of Justice authorized five agencies, including the Federal Bureau of Investigation (FBI) to deal with computer crimes (31) and the Internet, and the United States follows the United States in dealing with crimes Britain, which comes in third place after Sweden and America, passed the Anti-Forgery and Counterfeiting Law in 1981 AD, which included in its definitions of a forgery tool various computer storage media or any other device that is recorded, whether by traditional or (32) electronic methods or by any other means. Another way, Canada is ranked among this country that has given the face of cybercrime great care, is as it amended the Criminal Code in 1985 to include laws related to computer and Internet crimes, and the new law also included the renewal of penalties for computer violations and crimes of destruction, or illegal entry into computer systems, Or illegal entry into computer systems, as it clarified the authority of the investigation authorities as stated in the Competition Law, which authorizes the judicial arrest officer when he obtains a judicial order the right to inspect computer systems, deal with them and seize them. And here, Denmark has enacted its first laws on computer crimes and the Internet, which included paragraphs

for the specific penalties for computer crimes, such as illegal access to a computer, forgery, or any illegal gain, whether for the offender or a third party, or illegal manipulation of computer data such as destroying, expressing or making use of it. France has also taken care of developing its criminal laws to correspond with criminal developments. In 1988, it issued the law that added to the criminal computer crimes law computer crimes and the penalties prescribed for them, and its penal code was amended in 1994 to include a new set of legal rules for information crimes and assigned to the Public Prosecution the authority to investigate them, including a request for investigations and hearings sayings (33). There are also laws in the Netherlands, Japan and Poland related to computer and Internet crimes that explain how to deal with these crimes and the defendants in them, or those laws give the accused the right not to print computer records, or divulge passwords or codes for programs, and also give the witness the right to Refrain from printing information retrieved from the computer whenever this leads to his conviction or the conviction of one of his relatives. Rather, the criminal laws in force in Poland go further than this, as they stipulate that no coercive action or interpretation of this should be matched to the detriment of this accused and at the level of Arab countries We find that the Egyptian law strives to apply the rules of the traditional criminal law to information crimes, which impose a kind of criminal protection against acts similar to the acts that form the elements of traditional crime, for example, that the patent law applies to the physical aspect of the automated information

processing system, and the texts of the Law have been adapted Protection of private life and the law criminalizing disclosing secrets so that it can be applied to some information crimes, and the criminal judiciary has been entrusted with looking into a cases that are committed against or by the media of information systems, as well as the case for the Kingdom of Bahrain, there are no laws relating to Internet crimes, and if there is a text close to the committed act, the stipulated punishment does not match the extent of the damages resulting from the Internet crime (34). As well as most Arab countries, including the Kingdom of Saudi Arabia, and all countries can confront these crimes by following the following: -

1- International cooperation in combating crimes.

2- Block pornographic websites.

3-Establishing new departments in the Ministry of Interior responsible for confronting these crimes.

4- Activating the role of the media in raising awareness.

Conclusion

Internet crime is all illegal behaviour that is carried out using electronic devices, resulting in the criminal obtaining material or moral benefits with the victim bearing a corresponding loss, and the goal of these crimes is often piracy to steal or destroy the information or spread a certain thought. Internet crimes, like other crimes, require the availability of the agreed-upon pillars for the necessity of their implementation and for them to exist on the ground. Therefore, the material pillar, the moral pillar and the legal pillar must be present. The material pillar is criminal behaviour that results in a harmful result for the victim. As for the moral element, it is the intentional intention of the criminal through planning to commit the crime. As for the legal pillar, it is the unlawful act of the behaviour carried out by the criminal by performing an act or abstaining from an act. Internet crimes have many forms, including its use in the service of terrorist organizations by promoting them, including members to them, communicating with them, and using it in the drug trade by displaying and promoting illegal goods, and using the Internet in pornographic, immoral and sexual crimes from among others by displaying sexual images and inviting adults and children to have sex and using social media to impersonate the person to benefit from that identity or facilitate the commission of the crime. Since Internet crime is the most dangerous, prominent and most common crime, countries have raced to legislate laws to reduce it and protect national security and the privacy of individuals and the security of companies, including the Iraqi legislator in the Information Crimes Law of 2011, but it is still not able to reduce this crime and lies in it Many gaps, but Sweden was the first to enact computer crime legislation in 1973Which treats cases of computer fraud in addition to including general paragraphs that include crimes of illegal access to computer data, forgery, transfer or illegal access to it, The United States of America came after Sweden, where it enacted a law on the protection of computer systems from 1976-1985, and in 1985 the National Justice Institute identified five main types of information crimes. These are

internal computer crimes, crimes of illegal remote use, computer tampering crimes, support for criminal transactions, and theft of ready-made programs and hardware components of the computer. There are also laws in the Netherlands, Japan and Poland for computer and Internet crimes that explain how to deal with those crimes and those accused of them. If these laws give the accused person the right not to print computer records, or divulge passwords or codes for programs, and also give the witness the right to refrain from printing information retrieved from the computer whenever this leads to his conviction or the conviction of one of his relatives, and on At the level of Arab countries, we find that Egyptian law strives to apply the rules of traditional criminal law to information crimes, which impose a kind of criminal protection against acts similar to the acts that form the elements of traditional crime, as well as most Arab countries, including the Kingdom of Saudi Arabia. Despite this, the stipulated penalty is not commensurate with the extent of the damages resulting from Internet crime.

Results

1- Internet crime is one of the crimes that harm the national security of countries.

2- Internet crime is one of the crimes that affect the security of individuals.

3- Internet crime takes many forms, such as drug trafficking, impersonation, or Promoting terrorist organizations.

4- Countries are racing among each other to legislate laws to confront crimes that take place via the Internet and limit them and fill in the gaps in the current laws.

5- Iraqi legislation is deficient and incomplete in terms of limiting this crime and filling the gaps and in terms of deterring criminals.

6- The Arab legislation is not integrated and is weak in deterring the criminal.

Recommendation

1. We recommend to the legislator the need to benefit from the Arab and international experience in enacting laws regarding internet crime.
2. We recommend the legislator severely punish Internet crimes to deter hackers and reduce Internet crimes.
3. We recommend the need to spread awareness among people about the dangers of dealing with bad or suspicious sites on the Internet.
4. We recommend that competent authorities carry out awareness and educational campaigns for individuals regarding the protection of their devices and personal accounts from hacking and to enhance the security of their accounts.
5. We recommend that competent authorities train and rehabilitate criminal investigators on how to deal with

cybercrimes, collecting evidence, inspection, prosecution, investigation and inference.

1. Amir Farag Youssef, Information Crimes on the Internet, Alexandria University Press, 2008, p. 20.
2. Bahar, Abdul Rahman Muhammed, Obstacles to the Investigation of Internet Crimes, A Survey of Police Officers in the State of Bahrain, Unpublished Master's Thesis, Naif Arab University for Security Sciences, Riyadh - Saudi Arabia, (1420 AH), p. 2.
3. Al-Badayna, Diab, Computer and Internet Crimes, Researches of the Scientific Symposium to Study Modern Criminality and Ways to Confront it, Naif Arab University for Security Sciences, Tunis, 1420 AH, p. 98
4. Muhammed Mahmoud Mandora, Computer Crimes, Computer Virus Course, United Horizons Office, Riyadh, 1410 AH, p. 21
5. Article 28 of the amended Iraqi Penal Code No. 111 of 1969
6. Dr. Ali Hussein Al-Khalaf and Sultan Al-Shawi, General Principles in the Penal Code, Al-Resala Press, Kuwait, 1982, p. 139
7. Article 403 of the Iraqi Penal Code No. 111 of 1969, amended 139
8. Muhammed Amin Al-Rawhi, Computer and Internet Crimes, University Press, Alexandria, 2004, p. 123
9. Articles 361, 362, 363 of the amended Iraqi Penal Code No. 111 of 1969.
10. Omar Muhammed bin Younis, ibid, p. 298.
11. Hawra Rashid Mahdi al-Yasiri, Electronic Terrorism and Methods of Confrontation, Markaz al-Furat Newspaper, Issue (8386), 25/5/2017.
12. Omar Muhammed bin Younis, Crimes arising from the use of the Internet, Dar Al-Nahda Al-Arabiya, Cairo, 2004, p. 267.
13. Nabila Heba Harwal, Procedural Aspects of Internet Crimes, Dar al-Fikr al-Egamie, Alexandria, 2006, p. 49.
14. Muhammad bin Younis, ibid, p. 298.
15. Omar Muhammad bin Younis, ibid, p. 298.
16. Medhat Ramadan, Criminal Protection of Internet Sites and Their Contents, Legislation Journal, No. 2, Q1, 2005, p. 41
17. Counselor Amr Isa El-Fiqi, President of the Court (formerly), Computer and Internet Crimes in Egypt and Arab Countries, Modern University Office - Alexandria, 2006 - p. 102
18. https://www.hjc.iq/view.1645/
19. Hisham Abdel Qader, Information crimes from a legitimate and legal perspective, research published on the Internet without pagination.
20. Abdul Rahman Abdul Aziz Al Shunaqi, Information Security and Computer Crimes, 1st Edition, Riyadh, p. 18.
21. Ahmed Hossam Taha Tammam, Crimes Arising from the Use of Computers, Dar Al-Nahda Al-Arabiya, Cairo, p. 200.

22. Abd al-Rahman Muhammed Najd, Obstacles to the Investigation of Internet Crimes, A Survey of Police Officers in the State of Bahrain, Master's Thesis, Naif Arab University for Security Sciences in Riyadh, Saudi Arabia, 1440
23. The Iraqi Information Crimes Project Law for the year 2011 AD, unpublished.
24. The Iraqi Electronic Signature Project Law for the year 2011 AD, unpublished.
25. Article (26/First/D) stipulates: " The information is traced back to computer systems and networks in a suspicious position, provided that the authorities that own this system and networks are informed of the procedure and its scope, provided that the scope of this procedure is limited to the conduct under investigation without violating or prejudicing the rights of others."
26. This authority was transferred to the Supreme Judicial Council instead of the Ministry of Justice after the independence of the judiciary was announced, as the judiciary in Iraq was administratively linked to the Ministry of Justice, where the Minister of Justice assumes the presidency of the Council of Justice until the (dissolved) Coalition Provisional Authority issued Order No. (35)) for the year 2003 AD, and the text of section (6/2) of itas:
27. The Council of Judges replaces the Council of Justice, which was formed under the Judicial Organization Law (Law No. 160 of 1979 AD) and assumes the exercise of the authority that the Council of Justice used to exercise over any judge or public prosecutor. Published in Al-Waqa'a Al-Iraqiya, Issue 3980, September 2003 AD.
28. See: Article (73) of the Code of Criminal Procedure No. (23) of 1971 AD.
29. Dr. Khaled Mamdouh Ibrahim, The Art of Criminal Investigation in cyber Crimes, Dar Al-Fikr Egamie, Alexandria, 2009. , p. 207.
30. Dr. Thanon Ahmed, Explanation of the Iraqi Penal Code (General Provisions), 1st ed., vol.1, the Ministry of Information helped publish it, Baghdad, 1977 AD, p. 65.
31. Hisham Abdel Qader, Information crimes from a legitimate and legal perspective, research published on the Internet without pagination.
32. Abd al-Rahman Abd al-Aziz al-Shniqi, Information Security and Computer Crimes, 1st Edition, Riyadh, p. 18.
33. Ahmed Hossam Taha Tammam, Crimes Arising from the Use of Computers, Dar Al-Nahda Al-Arabiya, Cairo, p. 200.
34. Abdul Rahman Muhammad Najd, Obstacles to the Investigation of Internet Crimes, A Survey of Police Officers in the State of Bahrain, Master's Thesis, Naif Arab University for Security Sciences in Riyadh, Saudi Arabia, 1440.

References

1. Ahmed Hossam Taha Tammam, Crimes Arising from the Use of Computers, Dar Al-Nahda Al-Arabiya.
2. Amir Farag Youssef, Information Crimes on the Internet, Alexandria University Press, 2008.

3. Hassan Emad Makkawi, Communication Technology in the Information Age, 1st st Edition, The Egyptian Lebanese House, Cairo, 1993 A.D
4. Hawra Rashid Mahdi Al-Yasiri, Electronic Terrorism and Methods of Confrontation, Issue Center newspaper (8386), 25/5/2017
5. Khaled Mamdouh Ibrahim, The Art of Criminal Investigation in Cyber Crimes, Dar Al-Fikr Egamie, Alexandria, 2009.
6. Abd al-Rahman Muhammad Bahr, Obstacles to the Investigation of Internet Crimes, a survey study on Police Officers in the State of Bahrain, Unpublished Master's Thesis, Naif University For Security Sciences, Riyadh - Kingdom of Saudi Arabia.
7. Abd al-Rahman Abd al-Aziz al-Shniqi, Information Security and Computer Crimes, 1st Edition, Riyadh.
8. Abdul Rahman Muhammad Najd, Obstacles to the investigation of Internet crimes, a survey study on Police Officers in the State of Bahrain, Master's Thesis, Naif Arab University of Sciences Security in Riyadh, Saudi Arabia, 1440
9. Abdel-Fattah Bayoumi Hegazy, Electronic commerce and its legal protection, Dar Al-Fikr Egamie, Alexandria, 2004
10. Ali Hussein Al-Khalaf and Sultan Al-Shawi, General Principles in the Penal Code, Al-Resala Press, Kuwait, 1982.
11. Amr Isa El-Fiqi, President of the Court (Formerly), Computer Crimes And the Internet in Egypt and the Arab Countries, Modern University Office - Alexandria, 2006.
12. Omar Muhammad bin Younes, Crimes arising from the use of the Internet, Dar Al-Nahda Al-Arabiya , Cairo, 2004.
13. Theyab Al-Badayna - Computer and Internet Crimes, Researches of the Scientific Symposium for the Study of Criminality The new developments and ways to confront them, Naif Arab University for Security Sciences, Tunis, 1420 AH.
14. Thanoun Ahmed, Explanation of the Iraqi Penal Code (General Provisions), Volume 1, Part 1, helped Ministry of Information on its publication, Baghdad, 1977 AD.
15. Raouf Obeid, Principles of the General Section of Punitive Legislation, 3rd Edition, Dar Al-Fikr Al-Arabiya , Cairo, 1966 AD.
16. Muhammad Amin Al-Rawhi, Computer and Internet Crimes, Alexandria University Press, 2004.
17. Medhat Ramadan, Criminal Protection of Internet Sites and Their Contents, Legislation Journal, No. 2, 2005.
18. Mandora, Muhammad Mahmoud, Computer Crimes, Computer Virus Course, United Horizons Office, Riyadh, 1410 A.H.
19. Nabila Heba Harwal, Procedural Aspects of Internet Crimes, Dar Al-Fikr Egamie , Alexandria, 2006

20. Hisham Abdel Qader, Information Crimes from a Sharia and Legal Perspective, a research published in a network.

The laws

1. Iraqi amended Penal Code No. (111) of 1969
2. 2 - Code of Criminal Procedure No. (23) of 1971 AD
3. The Iraqi Project law on information crimes for the year 2011.
4. The Iraqi electronic signature bill for the year 2011.

The internet

1. https://www.ita.gov.om/iTAPortal_AR/Pages/Page Aspx?NID=1&PID=9&LID =5.
2. **https://www.hjc.iq/view.1645/**