IJTIHAD Journal On Legal and Economic Studies ISSN: 2335-1039
Volume: 10 Number: 01 Year 2021 P 32 - 50

Received:11/11/2020 Accepted:09/01/2021

ELECTRONIC CRIME

الجريمة الالكترونية

Mezaour nassima*[1]; Abdel Hamid DJEDID[2]
Ouled himouda djamaa[3]
[1]University of Ghardaia,(Algeria),
mezaour.nassima@gmail.com
[2]University of Ghardaia,(Algeria), djedidhdjedidh@yahoo.fr
[3]University of Ghardaia,(Algeria),
ouledhaimouda.djemaa@univ-ghardaia.dz

Abstract:
The technological development, especially in the electronic field, was a helping and facilitating issue of daily life, just as the emergence of the Internet facilitated things in an individual's life and shortened distances, as it helps him daily in accomplishing his research and scientific tasks, as it has facilitated his communication with all individuals around the world, in addition to the ability to book for travel and residence by pressing a button and following the news, shopping and other matters, but there is a negative aspect in its use, which is the criminal side, as some groups and individuals have used it to harm others, whether this harm is psychological, physical or material. It is used to steal money and personal information and the kidnapping of children and girls and all these heinous crimes are done remotely and this is what we will get to know.

Keywords: ELECTRONIC; CRIME

***Corresponding author**

الملخص:

إن التطور التكنولوجي خاصة في المجال الالكتروني كان أمرا مساعدا و مسهلا للحياة اليومية كما أن ظهور شبكة الأنترنت سهلت الأمور في حياة الفرد و قصرت المسافات إذ أنها تساعده يوميا في إنجاز مهامه البحثية و العلمية كما أنها سهلت عليه التواصل مع كل الأفراد في جميع أنحاء العالم إضافة إلى القدرة على الحجز للسفر و الإقامة عن طريق ضغطة زر ومتابعة الأخبار والتسوق وغيرها من الأمور غير أن هناك جانب سلبي في استعمالها و هو الجانب الاجرامي اذ أن بعض الفئات و الأفراد استعملوها لإلحاق الضرر بغيرهم سواء كان هذا الضرر نفسي أم جسمي أم مادي فهي تستعمل لسرقة الأموال و المعلومات الشخصية و استدراج الأطفال و الفتيات و كل هذه الجرائم الشنيعة تتم عن بعد و هذا ما سنتعرف عليه.

الكلمات المفتاحية: الجريمة، الالكترونية.

Definition of online crime:

The modernity that characterizes the electronic crime and the difference in legal and cultural systems between countries has led to the lack of agreement on a single term to denote it and this disagreement has led to not having developed a unified definition of this criminal phenomenon, for fear of limiting it to a narrow field (Al-Arian, 2004, page 43). To define cyber crime, the trends are divided into four:

On the basis of the method of committing the crime:

These definitions depend on the method of committing a crime, as long as the method of committing the crime is the computer or one of the related modern technology means, it is considered an internet crime (Chernaouti-Heli, 2010, p. 24). This includes the definition of the Office of Technology Assessment in the United States of America as crimes in which computer data and information programs play a major role(Al-Kaabi,page: 33).

It was also defined as: a criminal activity in which electronic technology (the digital computer and the Internet) is used,

directly or indirectly, as a means to carry out the targeted criminal act (Kahlouch, 2007, page 51).
Cybercrime is defined as those crimes resulting from the use of information and modern technology represented by the computer and the Internet in criminal acts and activities with the aim of achieving huge financial returns re-pumped into the international economy via the Internet using electronic money or debit cards that hold secret numbers by buying online or Stock trading and the practice of commercial activities via this network, and the experts of the European Organization for Economic Cooperation have expressed the crime of the Internet as being all unlawful, immoral or impermissible behavior linked to the automatic processing or transmission of data (Abdullah, 2007, Page 15).

Based on the availability of knowledge of information technology:
Supporters of this trend are based on a personal standard that requires the perpetrator of these crimes to be familiar with information technology (Ababneh, 2005, page 16):
The Ministry of Justice in the United States of America defined it as: Any crime for which the perpetrator has technical knowledge of computer technology enabling him to commit it (Al-Kaabi, page 34).
Professor David Thomson defined it as: Any crime that requires its perpetrator to have knowledge of computer technology (Rustem, 2000, page 407).

From the perspective of the owners of this trend, they required in defining the crime committed via the Internet, the availability of personal characteristics of the perpetrator, and they limited these features mainly to know-how and technical knowledge (Bozram, 2006, page 7).
Based on the subject of the crime:
The authors of this definition consider that the crime committed via the Internet is not the one that the information system is the

instrument of its commission, but rather it falls on it or on its scope (Al-Salami, 2010, page 63).
It was also known as: the crime committed via the Internet is the crime resulting from the introduction of false data in the systems and abuse of the outputs, in addition to other acts that constitute more complicated crimes from a technical point of view such as computer modification (Arab, 2002, page 8).

A trend that combines several definitions:
A crime in which a computer is used as a means or tool to commit it or is a temptation to do so, or a crime that the computer itself is a victim (Hayyan Al-Rashid, 2004, pp. 108-109).
It is any act or omission that would assault material or moral funds directly or indirectly as a result of the interference of information technology (Rustom, 2000, page 409).
It is all unlawful, immoral, or unauthorized behavior related to the automatic processing or transmission of data (Arabs, images of electronic crime and its classification trends, April 2006, page 7).
These definitions have been subjected to several criticisms because of their inaccuracy in defining the definition of the crime committed via the Internet, as it is sufficient according to these definitions that the behavior being social or immoral or against society so that it can be considered as a cyber crime and that these definitions depend on the description of the crime and not determining what it is nor it accommodates many of the criminal image that can be committed and the description of the crime is not considered one of the adequate disciplinary criteria for its adoption as a basis for determining what is the criminal act (Ababneh, 2005, page 19).
Note:
Information crimes have many names, including electronic crimes and crimes committed via the Internet.

Electronic crime characteristics:
It has six characteristics:

Concealment of crime and speed of development in its commission:
Crimes arising from the use of the Internet are characterized by being mostly hidden and hidden because the victim does not notice them, even though they may occur while he is on the network because the perpetrator has technical capabilities that enable him to murder accurately, for example when sending destructive viruses, stealing money or private data or destroying it, spying and stealing Calls and other crimes (Al-Kaabi, page 32).
Internet crimes mostly in all their forms are hidden not noticed by the victim or not even aware of their occurrence, and it is careful to block their behavior and hide it by invisible manipulation of electronic pulses or vibrations through which data is recorded is not in many cases due to the availability of knowledge and experience in the field of computers, most often among their perpetrators (Al-Mawasher, 2009, page 20).

Considering them less violent in implementation:
Cybercrime does not require violence to implement it or great effort, it is carried out with minimal effort compared to traditional crimes that require some kind of muscular effort that may be in the form of violence and abuse, as in the case of murder or kidnapping, or in the form of dislocation or breakage, and the copying of keys as it is the case in the crime of theft (Al-Badinah, 2006, page 20). All you need is the ability to deal with a computer at a technical level that is used to commit unlawful acts and you also need the presence of the International Information Network (Internet) with a criminal who employs his experience or ability to deal with the network to do various crimes such as espionage, breaching the privacy of others, or defrauding minors. In this sense, the crime committed via the Internet is considered among clean crimes. There are no traces in it of any violence or blood, but only numbers and data that are

changed from the records stored in the memory of computers and has no external physical impact (Abdullah Mohsen, 2007, page 52).

Transnational crime:

After the emergence of information networks, there are no longer visible or tangible boundaries that stand in the way of transferring information across different countries. The ability of computers and their networks to transfer large amounts of information and exchange them between systems separated by thousands of miles has led to a result that indicates that multiple places in different countries may be affected by one information crime at the same time (Mascala, 2000, p. 119).

The ease in the movement of information through modern technology systems made it possible to commit by means of a computer located in a particular country while the criminal act is being achieved in another country (Abdul Qadir al-Momani, 2008, page 51) and this is due to the fact that the information society does not recognize geographical borders, it is an open society through Networks that penetrate time and space without being subject to the border guards (Abdel-Qader Al-Momani, 2008, page 50).

Victims' failure to report:

Mostly, internet crimes are not reported either because the victim did not discover them, or because of fear of defamation, so we find that most of the internet crimes were discovered by chance, and even after a long time after they were committed, moreover, the crimes that were not discovered are much more than those revealed. It is revealed that the dark number between the truth about the number of these crimes committed and the number that was discovered is dangerous, in other words the gap between the number of these real crimes and what was discovered is a big one (Al-Adly, 2006, page 7).

This phenomenon is more apparent in financial institutions such as banks, savings institutions, lending and brokerage firms, where their boards of directors are usually afraid that negative publicity that may result from revealing these crimes or taking

judicial measures regarding them will erode trust in them on the part of those dealing with them and departing from them (Rustem, 2000, page 432)

The speed of erasing the evidence and the availability of technical means that impede access to it:

The data and information circulating via the internet are in the form of symbols stored on magnetic storage media that are only red by the computer and the identification of evidence that can be understood by reading and reaching through it to the perpetrator seems difficult, especially since the perpetrator intends not to leave a trace of his crime (El Azzouzi, 2010, p. 20) In addition to this, it requires a careful examination of the crime scene by specialists in this field to determine the possibility of evidence against the perpetrator and the subsequent examination of the vast amount of documents, information and data stored (Al-Kaabi, Page 38). As a criminal in cybercrime hinders investigative authorities, accessing evidence by the means such as scanning programs or putting passwords and symbols and may resort to encrypting instructions to prevent any evidence condemning him (scientists, 2004, page 877). It is easy to erase the evidence from the computer screen in record time by using the programs designated for that, as this is usually done in a blink of an eye and once light touch on the computer keyboard, given that the crime takes place in the form of orders issued to the device, and as soon as the perpetrator feels that his order will be revealed, he initiates the cancellation of these orders, which makes detecting the crime and identifying the perpetrator an extremely difficult matter (Arhumah, 2009, page 3).

Lack of experience with the security and judicial agencies and insufficient laws in force:

Cybercrime is characterized by many features that made it different from other crimes, which led to a comprehensive change in the investigation mechanism and methods of gathering evidence followed by the bodies that conduct the investigation process and adding burdens related to how to

detect this crime and its evidence, as well as the judiciary by amending many of its traditional concepts, whether in relation to evidence, its applications, or its power of proof (Mahmoud Hussein, 2008, page 58), as traditional laws are no longer able to keep pace with this tremendous speed in technology that led to the development of crime through it and the emergence of crimes that did not exist in the past, the existing traditional laws became not capable of confronting it (Al-Kaabi, page 40), which required the intervention of the legislator to enact modern laws to confront these crimes in order to preserve the principle of criminal legitimacy while strengthening cooperation between legal authorities and experts specialized in computer science, in addition to international cooperation to combat it (scientists, 2004, page 878).

Sectors targeted by online crime:

Financial and economic institutions:

Reliance on information networks has become almost absolute in the world of finance and business, which makes these networks due to their interconnected nature and openness to the world a tempting target for criminals, which increases the temptation of economic and financial goals is that they are significantly affected by prevailing impressions and expectations and doubting the validity of information or storing it in a simple manner can lead to devastating results and undermine confidence in the economic system. This situation includes causing a large disruption in the network systems that control the flow of the activities of banks and international financial markets and spreading chaos in international trade deals. In addition, a partial or total suspension of trade and business systems can be made so that economic activities are disrupted and stop working (the elephant, 2011, pages 92-93)

Natural persons:

Natural persons have become more victims of cybercrime, due to the continuous and large increase in the number of subscribers through the World Wide Web. The crimes committed via the internet are no longer limited to the financial

and military sectors, and therefore many people are subject to crimes of fraud, theft and destruction, and it is natural for the internet to be the fertile ground for committing these crimes, as millions of secrets related to people, whether they are ordinary individuals or in certain centers, are within reach of everyone who can penetrate the internet that contains all these secrets (Sheta, 2001, page 94) . The crime of violating private life is among the most common crimes across the Internet that natural persons are exposed to, and one of the most dangerous forms of these crimes are those that involve information stored in the computer after exploiting it for various purposes other than the goal for which it was collected, where the crime is the perpetrator's treatment of the electronic personal data intended to be used in a matter other than for which it was collected, such as that the statistical information is used to serve the tax authority for example, as well as the transfer or registration of private conversations is one of the crimes that affect private life, after the emergence of the Internet, it is possible to penetrate this Media, for eavesdropping and recording (Ababneh, 2005, page 72).

Military institutions:

The limits of the information revolution were not confined to the civil sector, but they were most important in the development of modern warfare systems and led to the emergence of the so-called information warfare, as this type of crime targets military and political goals, although it usually occurs rarely but it is present on the ground and the best example on that, the success of the Englishman (Nicholas Anderson) in penetrating the American naval website and stealing the special passwords used in the nuclear attack, as well as the success of the German (Hess Lander) in penetrating the Pentagon network database and was able to obtain 29 documents related to nuclear weapons (Syed Sultan, 2012, page 35).

Countries have taken the initiative to spy on other countries to obtain from them information that makes them able to confront them at any time by storming important military sites and viewing their data, and sometimes publishing this data on the

international information network, as happened in the penetration of the NASA network, The American Aerospace and Aviation Administration, hacked into the media site of the American "Sanya Waddage Debej" laboratory that works in the framework of nuclear weapons, as well as penetration of the main computer of the US Department of Defense and the publication of ballistic missile research (Hayyan Al-Rashid, 2004, page 149).

Categories of cyber criminals:

Pirate class:

Amateur hacker:

They mean adults who are fascinated by information technology and computers, and some of them are called small geniuses. Most of this group are students or young people who have knowledge in the field of information technology. The main motivator for this group is to enjoy playing and joking by using this technology to prove their skills and abilities by discovering and show weaknesses in information systems without causing any harm to them, they have the desire to adventure, challenge and discovery (Hegazy, 2006, page 46).

This group includes people who are targeting to enter into unauthorized computer systems to break security barriers established for this purpose in order to gain experience or out of curiosity or simply to prove the ability to penetrate these systems (Desouki Attia, 2009, page 180).

Opinions differed regarding the classification of this sect, as some believe that it does not seem appropriate to classify these young people into criminal sects because they simply have a tendency to adventure and a desire to discover, and their prohibited actions are rarely dishonest and they do not realize and do not appreciate at all the possible results that can lead to their unlawful actions in relation to the activity of a commercial establishment or company (Abdul Qadir Al-Momani, 2008, pp. 81-82).

Another team went on to consider these people as inferior to the criminals, because their behavior is simple and out of adventure

and challenge, they rarely do dishonest destructive acts and we are not afraid of them, they only aim to obtain information other than the professionals who aim to seize the data and unlike virus authors who aim to sabotage the information on computers.
As for the other team, it was pointed out that the actions of this sect are among the prohibited acts that are punishable by law in order to be able to combat this sect whose members may slip into the sects of cyber-crime professionals, in addition to the possibility of them joining the arms of dishonest organizations or individuals (Ababneh, 2005, page. 42).

Professional Pirates:

This group is known as adult criminals or professional saboteurs and their age ranges between 25-45 years. One of the most prominent features and characteristics of members of this community is that they have a place in society and that they are always specialists in the field of electronic technology, that is, they have skills and technical knowledge in the field of electronic and information systems that enable them to fully dominate the automated processing environment of information (Al-Hamid and Nino, 2007, page 73).

This category reflects their aggression, dangerous criminal tendencies that indicate their desire to cause sabotage, and these are distinguished by their wide technical capabilities and their experiences in the field of computer systems and networks, and they are more dangerous than the first category, they may cause great damage and usually the criminal offender via the Internet returns to the crime once again, his criminal record increases and he lives for many years from the proceeds of his crimes, and this criminal does not prefer extremist ideas but rather ideas that bring him personal profits (Al-Muwaisher, 2009, page 32).

The hatred sect:

This sect is often called the avengers because the character of revenge and revenge is what distinguishes it from the rest of the sects and is the motivator for their behavior because it is launched against the employers and establishments in which

they were working in retaliation against the employer for his miscalculation of them (Al-Minshawi, 2003, page 38).
The researchers believe that the goals and purposes of crime are not available to this sect. They do not aim to prove their technical capabilities and technical skills and do not want to achieve material or political gains and do not boast or speak out about their activities but rather they hide and deny their actions and there is no age group for them. And most of their activities are carried out by using virus and harmful programs techniques to sabotage information systems or destroy all or some of its data or targeted websites from the internet (Abdul Hafiz, page 34).
This group is classified in terms of ranking in criminal risk among the least dangerous sects among IT criminals, but that does not prevent some of their activities from causing huge losses to the institution they work with (Al-Malat, 2006, page 62).

The sect of intellectual extremists:
The difference between the East and the West, or between the North and the South, or between the Socialists and the Capitalists, or even between the different religions or sects of the same religion, contributed to highlighting this sect in the sense that each sect stokes ideas and opinions on the topics of the dispute with other sects regardless of the nature of these differences, whether religious, political or economical (Abdel Qader Momani, 2008, pages 85-86).

Class of spies:
Among the most important goals of this group in the use of information systems is to obtain information of enemies and friends alike in order to avoid evil or outweigh them, and military information is no longer the main goal, but rather includes economic, technical and industrial information (Merhej Al-Hiti, 2004, page 137).

The sect of system hackers:

Members of this community exchange information with each other in order to inform some of them of weaknesses in information systems. The process of exchanging information between them is carried out through electronic media releases such as newsgroups. Rather, members of this group conduct conferences for all infiltrators of information systems so that experts from among them are invited to consult about means of the breach and the mechanisms of its success and how to organize the work among them. The hackers follow several methods in distorting the pages of the sites. These methods differ from one site to another according to the type of operating system on which the site depends. For a different identity, exploiting security vulnerabilities in web servers, operating systems, and other methods (Omar bin Muhammad, 2010, pages 49-50).

Features of cyber criminals:

A cyber criminal has the skill of knowledge, mastery and intelligence:

Knowledge means getting to know all the circumstances surrounding the crime to be executed, the possibility of its success and the possibility of its failure. The perpetrators usually prepare to commit their crimes by identifying all the surrounding circumstances, to avoid unexpected things that would control their actions and reveal them, and the knowledge is distinguished by its previous concept, cyber criminals. Where a cybercriminal can fully visualize his crime (Desouki Attia, 2009, pp. 176-177).

Cyber criminals have a significant amount of skills in computer and internet technologies, but some of the perpetrators of these crimes are specialists in the field of processing information automatically. The implementation of the Internet crime requires a degree of skill with the actor who may acquire it through specialized study in this field or through experience acquired in Information Technology (Mascala, 2000, p. 118).

Intelligence is also considered one of the most important characteristics of the perpetrator of crimes through the Internet because that requires from him technical knowledge of how to enter computer systems and the ability to amend and change programs and commit crimes of theft and fraud and other crimes that require that the perpetrator should have a large degree of intelligence to be able to commit these crimes (Abdul Hafeez, page 13).

Internet criminal justifies the crime:

There is a feeling among the perpetrator of the internet crime act that what he is doing does not fall within the category of crimes, or in other words, this act cannot be characterized by immoral behavior, especially in cases where the behavior stands at the defeat of the computer system and bypassing the protection imposed on it, as the perpetrators of these crimes distinguish between harming people, which they consider extremely immoral and between harming an institution or entity in its economic capacity that can tolerate the results of their manipulation (Abdel-Qader Al-Momani, 2008, page 78)

Fear of revealing the crime:

The nature of the information systems themselves helps cyber criminals to maintain the confidentiality of their actions, because many of what exposes the criminal to discovering his command is that during the implementation of his crime, unexpected and unpredictable factors occur while the most important reasons that help the success of electronic crime are that computers rather performs their work often in an automatic way so that the various stages that any of their operations do not change from time to time , which help in not detecting the crime as long as all implementation steps are known in advance, as unexpected factors are not likely to interfere to reveal the crime (Al-Muwayshir 2009, p. 29).

The tendency to imitate:

The tendency to imitate reaches its maximum when the individual is located in a group, as it is then easier and more pleasant in the context of the influence of others on him, and this

appears in the field of crime committed via the Internet because most of the crimes take place from the individual's attempt to imitate others with the technical skills that he has which leads him to commit crimes. And there is no doubt that this is a result of the lack of leveling in the individual's personality, which is affected by the tendency to imitate due to the lack of controls that the individual inherits in himself, which impedes his instinct to interact with the surrounding environment, and ends up imitating and committing the crime (Abdul Hafiz, page 15).

Cybercrime objectives:

We can summarize some of the goals of cybercrime by a few points, the most important of which are: (Suleiman Al Harbi, 2013).

- ✓ Being able to access information illegally, such as stealing information, viewing it, deleting it, or amending it to achieve the criminal's goal.
- ✓ Web access to information providing servers and damaging them.
- ✓ Obtaining and blackmailing the confidential information of technology users such as corporations, banks, government agencies and individuals.
- ✓ Illegal material, moral or political gain through information technology such as hacking and demolishing websites, credit card fraud, bank account theft, etc...

Motives for committing electronic crimes: (Al Hyari, 2016)

Material motives: The objective that the perpetrator seeks is material benefit in order to satisfy the desire to achieve wealth

. Personal motives: They are as follows:

Learning: Hacking or hacking a site is a practical application of what a beginner has learned in hacking.

Revenge: It is considered the most harmful and one of the most dangerous causes that lead to the commission of electronic crime.

Mental causes: Its purpose is to demonstrate personal and technical capabilities in the ability to piracy.

Entertainment: and this type is without any motives or goals, and is only for the purpose of entertainment.

Political motives: The victim of political motives is usually the sites that adopt a policy against the government, or even simply by the difference of the political doctrine is a motive for penetration by the perpetrator.

Fighting and preventing electronic crime: (by presenting the research and discussing it in the classroom).

Download or buy an antivirus and make a permanent scan for your computer.

Avoid placing pictures and personal information on social media.

Reporting each suspect.

Adding new deterrent laws in the penal code to punish all perpetrators of information crimes and to protect victims.

Use the internet only when needed.

Permanent monitoring of children when using the Internet and explaining the danger to them.

Conclusion:

Through what we discussed, we see that electronic crimes are prevalent in all parts of the world and that it is the easiest way to carry out all the crimes mentioned before without the criminal being subject to arrest and investigation and thus must be prevented and that through guidance and guidance inside and outside the family as we should inform all members of society of their seriousness and the importance of reporting them, in addition to all this, the responsible authorities must strive more through developing technologies, enacting laws and applying them to everyone who commits this crime.

List of references:

List of Arabic references:

Ahmed Bouzram. (2006). Information crimes. Batna.

Ahmed Khalifa Al-Malat. (2006). Cybercrime (2nd edition). Alexandria: University House of Thought.

Al-Otaibi Omar bin Mohammed. (2010). Information security on websites and their compatibility with local and international standards. Thesis submitted to obtain a PhD in security science.

Riyadh: Naif Arab University for Security Sciences, College of Graduate Studies, Department of Administrative Sciences.
Ayman Abdul Hafiz. Technical and security trends to confront information crime. 2005.
Turki bin Abdul Rahman Al-Muwaisher. (2009). Building a security model to combat information crime and measuring its effectiveness. (College of Graduate Studies, Naif Arab University of security sciences, Editor) Riyadh.

Thiab Musa Al-Badayneh. (2006). the role of the security services in combating information terrorism crimes.
Sinai Abdullah Mohsen. (2007). Legislative confrontation for computer-related crime in light of international and national legislation. White House.
Tariq Ibrahim Al-Desouky Attia. (2009). Information security (the legal system for the protection of information). Alexandria: New University Publishing House.
Abdul Rahman Jamil Mahmud Hussein. (2008). Legal protection for computer programs. Palestine: An-Najah National University.
Abdel Fattah Hijazi. (2006). Principles of criminal procedures in computer and internet crimes (first edition release). Alexandria: University House of Thought.
Abdul Karim Abdullah Abdullah. (2007). Cybercrime and the Internet (Cybercrime) (first edition release). Beirut: Al-Halabi Human Rights Publications.
Ali Adnan Al-Fil. (2011). Electronic crime. Zain's Real Publications.
Ali Kahloush. (July 2007). Computer crimes and methods to confront them. (Directorate General of National Security, Editor) Police Magazine (84).
Ghazi Abdul Rahman Hayan Al-Rasheed. (2004). Legal protection from information crimes (computer and internet). Lebanon.
Muhammad bin Abdullah bin Ali Al-Minshawi. (2003). Cyber crime in Saudi society. Riyadh: Naif Arab Academy for Security Sciences.

Muhammad Hammad Merhej Al-Haiti. (2004). Modern technology and criminal law. Amman: House of Culture for Publishing and Distribution.
Muhammad Dabbas Al-Hamid, and Marco Ibrahim Nino. (2007). Protection of information systems (first edition release). Amman: Dar Al-Hamid for Publishing and Distribution.
Muhammad Syed Sultan. (2012). Legal issues in information security and electronic environment protection. Nashiri Electronic Publishing House.
Mohammed Saleh Al-Adly. (2006). Cybercrime (what it is and its images) the regional workshop on developing legislation in the field of cyber crime Muscat.
Muhammad Abdul Rahim Sultan scientists. (2004). Cybercrime and Accountability (3rd Edition). The United Arab Emirates.
Mohammed Obaid Al-Kaabi. Crimes arising from the unlawful use of the Internet. Cairo: Arab Renaissance House.
Muhammad Ali Al-Arian. (2004). Information crimes. Alexandria: New University House.
Mohamed Mohamed Sheta. (2001). The idea of criminal protection for computer programs. Alexandria: New University for Publishing.
Mahmoud Ahmed Ababneh. (2005). Computer crimes and their international dimensions. Jordan: House of Culture for Publishing and Distribution.
Mansour bin Saleh Al-Salami. (2010). Civilian responsible for violating privacy in the Saudi information crime system. Riyadh, Department of Criminal Justice: Naif Arab University for Security Sciences.
Musa Masoud Arohma. (2009). Procedural issues rose by transnational information crime. Tripoli.
Nahla Abdul Qadir Al-Momani. (2008). Cybercrime (First Edition). Amman: House of Culture for Publishing and Distribution.
Nahla Abdel-Qader Momani. (2008). Cybercrime (1st edition). Amman: House of Culture for Publishing and Distribution.
Hisham Muhammad Farid Rustom. (1-3 May, 2000). Information crimes: The origins of technical criminal

investigation and the proposal to establish a unified Arab mechanism for specialized training. Law, Computer and Internet Conference Research.

Younis Arab. (2002). Computer and Internet crimes (a summary of the concept, scope, characteristics, pictures, and rules of procedure for prosecution and proof). A working paper submitted to the Arab Security Conference. Abu Dhabi.

Younis Arab. (April 2006). Pictures of electronic crimes and their trends. Telecommunications Regulatory Authority, workshop on developing legislation in the field of combating cybercrime, Sultanate of Oman.

Foreign references:

Chernaouti-Heli, S. (2010). How to fight cybercrime? Science review (391).

El Azzouzi, A. (2010). Cybercrime in Morocco. Casablanca: bishop's solution.

Mascala, C. (2000). Crime and electronic contract. Paris.

Websites:

Iman Alhiyari. (January 14, 2016). Societal issues. Retrieved December 20, 2016, from a topic: http://mawdoo3.com/%D8%A3%D9%86%D9%88%D8%A7% D8%B9_%D8%A7%D9%84%D8%AC % D8% B1% D8% A7% D8% A6% D9% 85_% D8% A7% D9% 84% D8% A5% D9% 84% D9% 83% D8% AA% D8% B1% D9% 88% D9 % 86% D9% 8A% D8% A9 # .D8.AF.D9.88.D8.A7.D9.81.D8.B9_.D8.A7.D8.B1.D8.AA.D9. 83.D8. A7.D8.A8_.D8.A7.D9.84.D8.AC.D8.B1.D8

Sadeen Suleiman Al-Harbi. (October 28, 2013). Redemption Date December 20, 2016, from Law Firm: http://www.mohamah.net/answer/7211/%D8%A8%D8%AD%D 8%AB-%D9%84%D9%84%D9%83 % D8% A7% D8% AA% D8% A8% D8% A9-% D8% B3% D8% AF% D9% 8A% D9% 86-% D8% B3% D9% 84% D9% 8A% D9% 85 % D8% A7% D9% 86-% D8% A7% D9% 84% D8% AD% D8% B1% D8% A8% D9% 8A-% D8% B9% D9% 86-% D8% A7% D9% 84% D8% AC% D8% B1% D8% A7% D8% A6% D9% 85-% D8