CSCanada

Canadian Social Science
Vol. 10, No. 1, 2014, pp. 141-148
DOI:10.3968/j.css.1923669720141001.2789

ISSN 1712-8056[Print]
ISSN 1923-6697[Online]
www.cscanada.net
www.cscanada.org

The Legal Framework of Electronic Data Crimes

Shayma Muhammed Saeed[a]; Ali Ahmad Al Zubi[a],*

[a]PhD. Law School, Albalqa Applied University, Amman, Jordan.
*Corresponding author.

Received 20 October 2013; accepted 16 February 2014

Abstract

In order to determine the legal framework of these crimes, we should distinguish between two types of crimes or attack electronic data, the first type when the technology of electronic data process and telecommunication have used in remote to commit crimes. In other words these crimes are committed through computer and the criminal description of these businesses belongs to the known of types of traditional crimes like theft, fraud and other crimes. This type of crimes call un informatics in the global information network " internet" also this field includes the crimes of usage of "internet" and electronic data processes tools to show the pornographic images or diffusion a messages which are inciting to racism, racial, religious, discrimination or exposure to the personal liberty or intellectual property. The second types of electronic data process crimes when the technology of the electronic data and telecommunications are on remote and make it as a means of this crimes and their purpose too. And now we are in front of anew criminal acts which associated mostly to the exposure of security and integrity of electronic data systems and the confidentiality of the data and information that consist on. And this type of criminal information network called "internet", this is done in the case of illegal entry in to these systems and exposure to it or to the information that contain it. So this research will base on the electronic data crimes which are connected to the internet, when it becomes a direct target and a goal in their contents, and regardless on the impulsive of behind of committing.

Key words: Legal framework; Data crimes

Shayma Muhammed Saeed, Ali Ahmad Al Zubi (2014). The Legal Framework of Electronic Data Crimes. *Canadian Social Science*, *10*(1), 141-148. Available from: http://www.cscanada.net/index.php/css/article/view/j.css.1923669720141001.2789
DOI: http://dx.doi.org/10.3968/j.css.1923669720141001.2789

INTRODUCTION

The legal framework of electronic data crimes appear by depending on the statements of the types of the crime, especially when the computer became the mainstay of the objectives and developments of all the life domains over the past decades, which includes different activities whether economic, or scientific, or social …etc. the steady usage of electronic data performed whether in the form of money of electronic data or updated styles which help in manifestation of what is called of electronic data criminality. This is inevitable result for of scientific progress or technical novelty, this type of criminality based on several figures but what is important are two figures, one of them against money and the other one against people and it derives their activities from the huge potential of the computer. The computer himself is described as a tool of storage and he has the ability to store, organizing and exploiting unspecified number of information, and in the ame time he has the ability to get the information back in a short period of time and this information could be nominal. The punitive traditional laws are deficit to containment these criminal phenomenon. So before we come to these crimes we should offer the legal sides of these phenomena to take in to consideration when to decide any punitive policy. To settle this critical legal discussion in this field and to insure the safety of the information systems and security in the framework of using modern technology in the electronic data and telecommunication especially information network "internet" the crimes of attacking the information technology require a special rules and texts incriminating this new types of crimes.

1. THE CONCEPT OF ELECTRONIC DATA CRIME

We will show in this context the definition of electronic data crime or what we call informatics criminality and we will stop on the prominent characteristics which are characterized by this definition.

A-Definition of electronic data crime: before we give the definition of electronic data crime we should give a clear idea about the intended information and what we call now in the banks information and specify the legal characteristics because this information take a privilege place in this present age and it's the basic point in the discussion that associated to the informatics and it described as a science of information processing, even they said that the knowledge is authority, as some of them enhance that (1) its naturally familiar to depend efficiency in making any decision by depending on lots of available information and provide information in any moment to identify any country through their own thought or their science. Actually the information which is stored through the information network of it, it has a special legal nature, but if it has legal characteristics, it would be a subject of legal protection but in spite of what is stated in the bibliographies, and special books in this field in the definition of information or the information. But even this moment there is no legal text gives a comprehensive definition for it, the information in general is the raw material which through it can be preparing the thoughts to deliver it to the others. Depending on the previous explanation we notice that there is a difference between information and data, data is a set of facts or a measurements or data which take a picture of numbers, or letters or symbols or special symbols. It described an idea or theme or theme or specific target. So it described as a raw material which is converted through the computer for extracting certain information and the relation between the information and data called feedback cycle. It is assembled and operating data to get on the information then this information used in issuance a decisions which lead to an extra of data that collected and processed it again to get extra information again which relied on issuing a new decisions (2). Based on the information above we notice that the system of information cannot put accurate limit between what is called (input) and between what is called (output) because the interference between them are exist, what is call information in some stages or cases, it call data in other stages if it has been processed. Depending on our humble decision the information is a certain products and ideas which viable to temporary ownership by the beneficiary, it means it is independent of the service and it has nothing to do with the deed (machine) or the service that performed it. Therefore these information is capable for possess, so these information is a intellectual property and the products of its owner, whether its created by natural man or moral person unless if there is an agreement in According to the general rules of the intellectual property and literature furthermore that the information present to the owner personal and economic interests, in other words it has a positive impact to the people who are beneficiary of it. If the information is an idea is an idea or a group of ideas which has no boundaries, so it requires a special legal regulation. Therefore the information term is different from informatics or electronic data term, the last one means a science which associated to process a logical information that becomes a pillar of the knowledge of humanitarian and communication in the artistic, economic and social fields by using equipment mechanism, and the information system definition is all the special means create the information and process it for storage or to display it or destroy it. To operate it again it requires the use of another form or the recent of electronic means. We give a clear picture about the concept of information and informatics (electronic data) and the natural features of it and the legal too. It should be noted that the meaning of information banks are forming of database which are useful for particular subject and aims to serve particular purpose and processed it through electronic computing to out put it in a picture of regulating information which are useful for the users and provide them the advice in certain things, so we can say there is a bank of financial information or legal or medical or political or military or security and its possible that the information bank includes on more than one type of the previous types of data such as the national information banks. (1) The intended of electronic data system in the information network "internet" it is the equipment and informatics machinery, computers machinery, programs and rules of data banks (2) and websites. Discussion forums, news groups, and all informatics means which are special to industry, or processing or storage or retrieval or to view or transfer or exchange the information. Because of that and a result of increasing many aspects of oppressor exploitation and action which are associated with the use of bad faith performance of information processing, there is something appeared and it called informatics criminal and it describes as one of the multi faced for influenced attacking on the technology in the field of business and management and its not intended just as a theoretical problem in a future society which is governed by the information, but the information criminality is a social and material truth which make lots of scholars and researchers are busy in this field. What ever the case is, we should resist any hostile attitude towards the revolution of technical machinery process for the information which has great benefits. The beginning of the phenomenon of information criminality which has become the subject of researches in more details in the recent time (1). In the sixties of the last century when the newspapers and scientific books published of what called criminality of information technology which are related to the manipulating computer and defusing it and espionage on it and the illegal usage of it. It becomes so difficult to know whether these informatics crimes related to the facts or fiction and it's difficult to put a certain definition for the phenomena of the criminality creativity as a fear of confined in a narrow range especially because there is no agreement on this term to refer on this criminality creativity phenomenon. Some of them call it informatics fraud or "informatics crime" or information embezzlement and some of them call it computer crimes (2) and other of terms, however, it requires a reference to give a wide comprehensive definition which includes the basic elements that allow specifying these phenomena which becomes the research object. Therefore we will refer to the situation of the jurisprudence in determining the definition of electronic data crime, it includes any crimes against money and it belongs to the usage of processing of information or as a legal attacking which committed by informatics and the purpose is to achieve profit, and other identify it more widely because they want to present all kinds of the abuse in using information technology field. In their points of view they believe "every deliberately act or whatever which relate to the informatics, and creates a loss which incurred of the victim or gain derived by the actor, or it's all the forms of illegal behaviors or which it's harmful to the society or an illegal act which used the computer as a major tool (3). We noticed from the previous definitions that some of them focuses on linking of crime with the achieved of money it means linking the base of penal code with the purpose of act, but the originality of criminalization has nothing to do with the purpose because its not an element of it and then the default of electronic data crimes on the cases which the criminal intended to achieve profit in illogical way, this type of crimes could be committed but it has no relation with the profit like the crimes of espionage and seeing on the information or discover a trade secrets or abuse to the reputation and other crimes which are related to the same subject matter of the research. The definition of electronic data crime, it's a set of action which are associated with the informatics that can be worthy of punishment while its known also from the jurisprudence field as a group of crimes which are related to the logical process science while the other side identify it as any act which are created on the illegal usage of information technology and it aims to attacking of physical or moral money and its clear from these definitions that its more sense than the predecessor for trying to avoid the advance criticism like exclusion the criminal act which are committed in the occasion of using of computers, as well as the exclusive of the motive or purpose of doing these acts is making profit and we can say that the electronic data crimes which are happened on the special legal nature which are distinguish on the other part of traditional crimes, furthermore, the characteristics and other features of it, it seems the doubt is clear about the ability of penal laws of this phenomenon and them applying the general texts rules to protect the moral values which are created on the electronic data.

2. THE MAIN CHARACTERISTICS OF ELECTRONIC DATA CRIMES

As a result of the internal circulation of the programmed data which are crosses the countries (international transport)and circulation the simple information (un programmed) and the speed of circulation information network, all these things led to technical change in this field to ease the circulation of information in this field, then it help in committed electronic data crime through the personal computer or other computers which are used in a certain countries, in spite of the result of crime which has been achieved in another countries. So the electronic data crime becomes a new form of cross border crimes and in this way it takes a forma which can be distinguished on other crimes (1). It could be mention some features that can be made the electronic data is general and committed on the network information is special, and its different from other traditional crimes, they are as follows: **a)** It's a transient countries crimes (transnational crimes) the crimes which are happened between more than one country, it means that it don't confess of the geographical borders of the countries, such as money laundering and drugs and others. Mostly the culprit in country and the victim in another country, and it may also the potential damage in a third country in the same time, so the informatics crime becomes the new form of cross-border crimes of national or regional. **b)** It's a crimes which are difficult of proof, its difficult in many cases to find the material impact of the electronic data crime, perhaps the reason behind that is the culprit often uses a technical complex means, and the behavior of the former is very quick act, and it doesn't take more than few seconds, in addition of erase the evidence and manipulate it, in this time this type of crime are lacked to traditional physical evidence (blood, hair, fingerprint). **c)** Electronic data crime assets play that its less violent than the traditional crimes, i.e., it doesn't need to the effort muscle, but it depends on the mental expertise and studied scientific thinking which based on the knowledge of computer techniques, so it calls a soft crimes. In fact there is no feeling of secure about criminals in the field of mechanic process information because the perpetrators are not professional in criminality as they are known (1). **d)** The motive to commit electronic data crimes is different from the traditional crimes, in the first group the motive is to breach the public orders and out of laws are more targeting to get profit, we notice that the motivation with perpetrators with the second group in general is to get money (2). But if the motivation combine with electronic data crimes committed in order to achieve the physical benefits, the amount of money would be too huge. **e)**

Ordinary crimes are classified in the most legislation according to what the jurisprudence believe, money crimes and people crimes, but electronic data crimes are classified to multi criteria and the most important of it are follows:

A. Legislative classification and it takes one of these forms:

a. illegal usage of tools which are connected of computer

b. the destruction or modification of information or files

c. theft of money or financial documents and valuable data

B. Classification based on the type of use which is called a logical types and it the crimes classified as follows:

a. Modification and destruction

b. Usage and Deniable, this category contains many types of crimes (disorganization, tapping, trapping and interception of data.)

C. Classification based on the crime, such as cheating, theft, espionage and attacking on the privacy **(1)**

3. THREE PEOPLE OF ELECTRONIC DATA CRIME

Electronic data crimes suppose to have perpetrator and victim, but the branches of the electronic data crime is different in some times from the rest of other crimes, so the essence of this research is about the acts and how we direct it, and there is no doubt that the natural person is prepare the opportunity to exploit this informatics mean, but is it ok when the information network connect between multiple computers, the case is different, public institution and banks and others, which have the personal characteristic value is expose to attack through this network information, although of multi means of protection, but its not active in front of these piracy of the information network.

3.1 The Perpetrator in the Electronic Data Crime (Informational Offender)

From the beginning we can say that the idea of the informatics offender is a new idea in criminal jurisprudence, we are not from a traditional criminal, but we are front of a criminal with technical skills and aware of usage techniques in the system of computers. The personality of the informatics offender whether natural or moral and his style in committed the crimes makes him a persona has a especial features which are available in the normal criminal, and what is make him distinguishing on the other criminals is his familiarity with the issues of informatics, and enough knowledge of the mechanism of the acting of computer and how it runs, electronic data criminality creates as a result of quiet destruction techniques like manipulate of information and the logical entities (2). Or data, but that does not mean the possibility of depicting the violence against the information system, it maybe the subject of the crime is damaging the computer itself, or the CPU (central process unit) which means that you can abuse it by structuring the computers not through the information that are on the information network. Whatever the mater is, there is no punishment to achieve the goal whether in the field of public deterrence or private deterrence unless if wee keep in our mind the characteristic of the offender even if we re qualification him socially to return to the society again good citizen, by considering the reform of the criminal is the main point in the modern punishment system (1). The informatics criminality becomes the smart of the crimes by comparing with the traditional crimes which are tends of the violence in spite of the violence criminality which are directed against the informatics system which is reflected what we have said the destruction about the computer. On the other hand we can say that the electronic data crime as a social phenomenon that has a result of factors in the mind of the perpetrators, many of these perpetrators are committed it just for fun or just to show their superiority on the machine or the security programs for information system without obtaining financial benefit or just proud of themselves and show to their victims the weakness of their security systems, and it's clear to say that there is a lack of social risks in the informatics crime and the reason of that there is no wicked intent but the unconscious of behavior which can cause a serious damage even if it doesn't reveal any hostility to the community, therefore the perpetrators of the informatics crime are not on one degree of risk or efficiency and on this basis we can classify them depending on their abilities and intention of the commission of the crime into two types:

a. Criminal users who have the enough knowledge or experience in the informatics field or the computer business and the components and the basic function of it and know some programs that are being worked like accounting program and recognizing that informatics are modern technology and their usage in the daily life is modern, as a result of lacking of the knowledge of these technology and when they practicing their talents for the purpose of access to the information for practicing their own hobby, and they don't realize the consequences that could be lead their illegal actions to any particular activity, therefore this set of class of criminal become less dangerous comparing with other, as we will see later, but with notice of increasing number of people who use this technology (Internet). What is followed undoubtedly of increasing the level of this crime in this field? It's not possible that this class would slide in these crimes as a hobby for the illegal acts to the professional in the crimes (1), especially if they are embrace from criminal organization to achieve dangerous purposes in one way or another on the scientific technology.

b. Criminal programmers: Because of the level of skills that the programmers enjoy of it from entering and or storming in to the computers systems in easy way and professionalism in spite of the multi precaution security and in spite of lack of the professional elements for detection it, it seems to be this class of criminals are clear too much, transfer crime, copying and adding information on the programs and changing the content of this category is a huge work (2). Furthermore people of this category be able to use possibilities and informatics methods not only in the commission of the crime but even in shirk to detect their heads or by working on obstruct them through wasting the evidences which are leading to make them guilty (3). Through the previous explanation above its clear to say that the offender of the informatics crime may be an active or a partner in the commission of the crime, the original feature of the perpetrator in the informatics crime often one of the workers or the users in the institutional which are managed by informatics system, regardless on the beneficiary of the commission of this acts, this type of crimes requires the precision and quick in doing the illegal operation. It requires a participation or help from other people, whether they are professional or just brokers. This participation could be negative, and it could be translate in silence. It is often that the technical helping requires a modern mechanism for deceiving the computer and use a set of intermediaries or partners or custodians of the computers CDs because those people play important roles in success these illegal operation or target operation. We should remain in this research that there are main concerns that motive those criminals to commit electronic data crime such as passion of electronics and personal motives related to the proof of greatness and prove the ability to drive profit and also there are external influenced coercion, malice or it could be for reasons of administrator particularly, a special reason of institution.

3.2 The Victim of the Informatics Crime

As the informatics crimes are committed by natural or legal person, the victim in those crimes might be natural or legal person, the majority of these crimes are on natural person who present institution and financial sectors and large companies, the infinitive information becomes in the modern time one of the most important target after the money, especially if these information are highly important and the objective of the offender is got money by illegal swapping for this information or sell it to the rightful owners. We can imagine that through the following information:

i. Financial information which are associated with the arithmetic, financial status, administrative and transmission money and investments (1).

ii. Business Information: especially with regard to e-commerce and espionage operations and piracy.

iii. Personal information its related to the natural or moral features like companies, hospitals, police stations, parties, association and others. Whether the information is stored in the computer memory, then it confuse it and showing it on the un reality, and this type has the secrets of the country, industrial projects which are associated of reinforcement war which is more important target from the other. Its noticed in this regard to the role of the victim in forbidding informatics crime, in the most part, the role of the victim is very small and negative, lots of victims prefer to keep what they happened with them secret, in other words, they conceal of the what they happened with them like the damage which are caused on the informatics crime and the reason behind that is to keep on the social status or their business reputation and to protect their financial status and customer confidence with them, they don't want to reveal of the breaches that occurring on their computers, so they will not looking at the security system and call it a weakness security system and are not active and make a kind of weak trust in the institution then the customers will reluctant on it. As well as the inability of the victim in the material proof of the crime, as well as the fear of the possibility of legal accountability, in a time which they have a duty to supervise the target information and having the necessary authority for the possibility to make the necessarily procedures in the even of damage which are arising from the disclosure of the information in the level of sensitive and risks (1). So the incidence in this field plays a very important role in reveals this type of crimes in my humble opinion this thing is true to some extent in our country, but in the western countries the consciousness in this field is very big, and the owners of the companies don't fear to announce on the breaches in their companies, to get their own right and punishment the criminals and it has a benefit to the judicial power to put the best solution to combat it in the future.

4. THE LEGAL NATURE OF ELECTRONIC DATA CRIME

There is no doubt that studying the crime in general and electronic data crime in a particular is under the scope of the study of the penal code, this branch is specialist in studying each crime separately and addressing the basic elements for each crime and the punishment for it (2) the electronic data crime is a criminality phenomenon that has a special nature associated to the informatics penal code, this type of crime committed with the scope of data processing whether in collecting, preparing it or enter it to the computer which are linked to the network information and to get a certain information, these crimes could be committed in the field of process words or processing texts, the last type of these crime is merely (automatic) that enables the user to edit documents and texts on the computer and providing the possibility of correction and amendment, scanning, storage, retrieval and printing. All these processes are close to the crime, so the offender has to assimilate it, as well as the offender may have to deal with new vocabulary such as programs and data which are using to attack the means for it. These crimes have a special nature, the ability of the unique of the information network (the Internet) to transfer and exchange the information which has a personal information like attacking on the personality freedom, and the reason behind that is the expansion of data banks, furthermore on the expansion of the people and their requests to link their computers to the network, which raises a question about the nature of services and the application in the net work in order to know the form of the texts and roles that you should apply it to the dissemination services sites and the exchange of information in general and in a particular understand the knowledge of the legal system of responsibility which is supposed to apply to the people who are responsible for this publication or exchanges. In other words, can we describe the services and application in the information network, and it is under controlling of the postal service or spying or within the concept of press and publication or audio visual aids or television institution or radio (1) in any cases should we consider that the network information " internet" anew space of information, and it has no relation with the knowledge of post and telecommunications, nor the press, and hearing aids and radio and television broadcasting and then the general rules and principles about the liability which applicable to the service and applications too. The investigation of the appropriate nature of the legal system through the information network aims to know what is the legal texts that should be applied to the dissemination services websites and information which are in it, as well as the knowledge of the legal system of responsibility that supposed to be applied on the people who are responsible on this publication, specially to know the attitude of those countries about this matter, based on what we have before, the legal nature of this crimes become clear through the area that can be committed and on the other side the place of the commission which be attacked. Its clear that the rapid development in the field of electronic data and it may allow for the acquisition of electronic mean which helps the abusers to enable to used it in commission different crimes like the attacking of personality freedom (2) and there is no doubt that the electronic data criminality related to the wrongful conduct, and with regard to automatic processing of data and input the information and transfer it, and then its necessary to attach to the scope of the criminal law, in spite of that the most of comparison texts are unable to keep the new development in the information or what the legislative vacuum in this field. On the other hand these crimes have a special nature in the term of their legal and the traditional rules were not special to these criminal developed, traditional rules have a specific criteria (copied and material) while the concept of personal rights in the network information is the product of human thought, and its related to the human characteristic, money and property and the application traditional texts on the electronic data crimes which raises many problems like the issue of proof (1) such as getting material impact, the offender can erase the evidences of condemnation and destruction in a short time, especially in the case of inspections network or intercept process communication and the search on data could be encrypted and no one can know the code of entrance only the workers on the network, from this point there is a question is raised about the issue of legality to decode it (2). What is made it more difficult is chasing the offenders of the electronic data crimes "internet" who reside in another countries, which has no agreement of the country that investigates in a criminal behavior or a part of it, in the light of the above consideration we can be sure that these crime has a special legal crime that are committed by people who are committed it and they have a special skills and ruled by a special legal texts.

CONCLUSION

I. Deduction

(a) On the top of these results there is a report of legal protection of information, it requires special legal system that determines the dimension of it and decides their impacts.

(b) The information may has been exploited illegally such as distorted it or change it or trade it on illegal way.

(c) The information study requires a technical knowledge to have the subject and its dimension too to give a useful imagination serve the legal search in understanding the mechanism of network information and contribute to understand the possibility of making a legal rules that are adapt with this mechanism.

(d) The legal framework of electronic data crimes does not have enough study and interpretation in the jurisprudence criminal only in a recent time. So it was not a subject of special legal organization except in the western legal comparison, in this way the characterized by subjectivity in the tem of legal formulas and in the term of roles nature that should be subjective to them and their different impacts.

(e) The informatics danger increased as far as the evolution in the informatics field, in this way the same evolution depends on the availability success of the legal roles that are necessary for protection or failure.

(f) As we have seen in a time that we have believed the information protection has a relation with the definition that determined it, that the contemporary legal thought did not settle on one opinion that clarifies the definition of the information or demonstrating features, as well as the different legislation that don't have a specific text or context that we refer to it. It means that it's a boundless ideas and it requires a special legal regulation for it.

(g) We cannot depend on one legal system to protect the information because the different of transit through the global network "Internet" and because of the beneficiary and multi parts of it, it should be there a multi legal protection system.

(h) The electronic data crimes on the world wide web "internet" has a special nature unlike other traditional crimes, and it has derived this special nature that can be committed in it or the location which can be attacked from it.

(i) We found that the perpetrator of the crime or as some calling him (informational offender) who has advance technical empirical skills and aware of technical usage in the computers system, and he knows how to use the information systems, some of them describe this type of crimes as smart crime, because the perpetrators use a complex technical means. The material behavior for this part is very fast and it takes a few seconds and it's easy to erase the evidence, the informatics crimes are less violent than the traditional crimes, because it doesn't need a muscle effort but it depends on the intellectual knowledge and scientific thought which based on the technical of the computers so some of them calling it the soft crime or white-collar crimes.

II. Recommendation

As a result of the previous explanation the informatics age has needed to create a modern legal rules to face the crimes which are arising from the technology of information system for two reasons:

First, the updating forms of the electronic data crimes is not limited on the material values but it extent to include the moral values.

Second, what the information systems has been developed and the new means to commit the crime, that the traditional crime texts are unable to contain it, so we recommend some legislation that guarantee some rules that should be of it, and they are follows:

(a) The need of keep up with the criminal law in two ways, subjective and procedural to the phenomenon of electronic data crime, because there is a legislation lack on the criminality protection of the personal freedom. On the other hand inability of criminality proceeding in investigating the criminal case for crime information especially when it comes to storing data from abroad through the dimensional communication network.

(b) We recommend the comparative legislation to recognize the importance of informatics legal. By stopping these committed crimes on it, by text on their criminality and submitting these roles without relying on the penal code texts. These types of crime should be known widely to include the access illegal data process system programs and copy the information then disclosure it and use it on the illegal way and the emphasizes punishment on use it without a license or to be a subject of vampirism.

(c) Adopting a system which can be processed the output of the computer and the stored electronic license and accepted it in the judicial argument.

(d) Preventing the input of information that has a confidential nature on the basis of the religious nature, sectarian partisan union and ethnic. Since if these information is entered to the computer and record it, it could be a source of big problem, if there are events of sectarian and find out the information it could be a tool of implementation of other crimes or easy to commit it, what is requires here is to create a special legislative that organized of the use of electronic computers and information banks.

(e) Subjecting persons who are involved in collecting these information in duty of secrecy of these information.

(f) Subjecting people who are responsible on the computers to criminal penalties in the event of disclosure of confidential information and safeguard to the personal freedom, whether it belong to the individuals or legal persons.

(g) To give the concern persons who are involved to collect the information the right to review the administrative and judicial authorities to oblige people who work on the computer to implement their own rights.

(h) To make an effective facing to the global information network "internet" countries should have legislation in extradition and mutual legal offenders and exchange the judicial helping in the legal matters. The consistency of the concept of crimes of this kind of crimes that belongs to the internet, could be decisive in the matter of extradition the offenders, as well as the procedural problems that happened by modern technology and it could not be solved through the international agreements.

(i) It's enough for us to recommend in this whole research and this recommendation perhaps like a legal guarantee and it text on forming a special court from professional judges and experience in this field, and familiar with the technical means to operate these devices and the security means in it, to safe the rules that are issued on the court in violent the special rules of electronic personal data.

REFERENCES

Abdel-Rahman, K. H. (1992). *The legal protection of logical entities* (information programs) (Unpublished doctoral thesis) (p.60). Faculty of Law, University of Ain Shams, Cairo.

Abdullah, K. O. (1942). *The criminal protection of private life and data banks* (p.48). ED3, Al Nahda Al Arabyeh, Cairo.

Ahmed, H. A. E. (1997). *Witness commitment in the media of electronic data crimes: A comparative study* (p.66). Dar Al Nahda Al Arabeyah, Cairo.

Al Cheniqi, A. R. (1993). Security confrontation of computer crimes. *Life and Security Magazine, 11*(129), p.46.

Al Kareeb, I. N. (1994). *The security of computer and law* (p.81). Dar Alratib Al Jameiyah, Beirut.

Al kbasi, A. S. (1999). *Criminal liability from the use of computer, al maiedah al hurrah series* (p.127). The Seminar of Law and Computer, bayt al hekmah.

Al Khater, S. H. (1999). Contracts guarantees for the transfer of information. *Journal of Law, 3*(3), 121.

Al Saqeer, J. A. B. (2001). *Criminal confrontation to paid television programs piracy* (p.11). Dar Al Nahda Al Arabeyah, Cairo.

Al-Faruq Al-Husseini, O. (1995). *The important problems in computer-related crimes and international dimensions* (2nd ed.) (p.127). Cairo.

Almnaash, O. A., et al. (1992). Computer crimes and Internet (p.72). *Computer crimes in the comparison legislation*.

Alois, M. (1983). *The impact of technological development on public freedoms* (p.46). Al Maarif Institution, Alexandria.

Al-Shawa, M. S. (1994). *Information revolution and their reflection to the penal code* (p.173). Dar Al Nahdah Al Arabia, Cairo.

Awad, M. M. (1993). Contemporary criminal policy problems in information systems crimes (p.6). Paper submitted by Sixth Conference of the Egyptian Criminal Law, Cairo.

Bakri, S. H. (1990). Networks and employment information against crime. *Arab Journal for Security Studies and Training*, *6*(11), p.210.

Baqi, J. A. (1992). *Criminal law and modern technology* (p.16). Dar al nahdah al arabeyah, Cairo.

Ismail, R. (1999). The preventive of crimes which are arising from the use of computer. *Islamic Economics Journal*, (219), 34.

Jameel, A. B. (1999). *Internet, and criminal law, the subjective rules of crimes which belong to the Internet* (p.177). Dar Al Nahda Al Arabeyah, Cairo.

Kashoosh, & Hamid, H. (1992). *Computer crimes in the comparison legislation* (p.1). Dar Al Nahda Al Arabeyah, Cairo.

Muti kayal, M. S. A.. (1998). *The Internet and some of the legal aspects* (p.12). Dar Al Nahda library, Cairo.

Ramadan, M. A. H. (2001). *The criminal protection of electronic commerce: A comparative study* (p.35). Dar Al Nahda Al arabeyah, Cairo.

Rustam, H. M. F. (1992). *The penal code and the risks of information technology* (p.24). AL Allat Al Hadeetha Library, Assiut.

Rustom, H. (1999). The technical origins of the criminal investigation. *Journal of Security and Law*, (2), 110.

Sageer, J. A. B. (2001). *The procedural aspects of crimes, related to the Internet* (p.4). Dar Al Nahdah Al Arabeyah, Cairo.

Shamboor, T., et al. (1993). *Banking secrecy* (p.82). Research and discussions of the seminar organized by the Federation of Arab banks, Lebanon.

Shuqayr, R. S. (1997). *Computer data attacking crimes. (Unpublished master's thesis)* (p.10). Faculty of Law, University of Mosul.