

**Research Article**

## **Impact of E-Legislation in Securing and Defending the Knowledge Society**

**Abdulnaser S. H. Al-MSloun, Ph.D**

Faculty of Business, University of Jeddah

Jeddah, Saudi Arabia

**E-mail:** dr.abdulnaser@uj.edu.sa

[Received-25/08/2016, Accepted-06/09/2016, Published-11/09/2016]

### **ABSTRACT**

With the development of the digital age and the growing efforts to build knowledge of modern society emerged the need to develop the electronic legislation (cyber) deal with the legal issues arising from the use of information and communication and its various applications in the economic and social life, technology has become the technology used in scientific applications in e-business and government services and in the interactions different between individuals and institutions in order to legitimize electronic trading on the one hand and the statement of its controls and limitations and to protect the customers of the other hand on this cyberspace (cyber) has made many countries to issue private electronic transactions and commerce laws. This article focuses on discussing the various issues related to the privacy issues and data of a personal nature and in order of the sensitive nature of the protection of this data it was necessary to establish laws for the protection of personal information as well as the protection of all information that have the status of privacy and mutual either e-mail or through other social applications by preventing mediators from the use of this information without the owner's permission or misuse or placed inappropriately.

**Keywords:** ICT, Cyber, E-legislation, Crime, Intrusion Detection System, Privacy and social Life.

### **1. INTRODUCTION**

The cornerstone of the initial and necessary for Informatics and Computer is supposed. We cannot talk about the information without talking about this vital organ sheer invention which is known to mankind in the late twentieth century. Computer is one of the distinctive features of the present era. It uses closer system developed nations and societies aspiring to live with the concepts and methods of atheist century Twenty, considered a driving tool for the components of the cultural renaissance, particularly in the areas of education and the means of production and communication, trade, defense and information systems and other aspects and needs of its infrastructure. This is due to the rise and stunning massive and continuous development of software defined minimum in

recent years and progress in ultra-miniature electronics and software design, construction and storage of information technologies [1].

The need for legislation information required for cultural, scientific, educational and informational role, played by the information centers in the evolution of society and advancement, where is this legislation, a prerequisite for the success of any plan to organize or expand the services offered by information facilities, there must be laws and regulations governing the informational work, and define the duties and business information facilities internally, and its relation with each other. In developing countries, including Saudi Arabia (for example) need to be more pressing for such legislation, which is of the

most basic elements of national policy for information systems and services. These important initiated states and international scientific bodies to actively seek to pass laws and regulations and legislation to facilities of various information, designed to organize and codify and unify informational action at the national and global levels, the UNESCO has called for greater attention to legislation Informatics, in numerous conferences and seminars regional and global, and issued recommendations many in this regard [1-3]. Legislation and information laws plays an important role in ensuring the security of the information revealed gaps in the laws and regulations of information and knowledge in the Kingdom of Saudi Arabia and support developed to be a support to the trends and plans for the state to shift to the knowledge society in order to serve the Saudi community service and contribute to the renaissance at the regional and international level. The eighties had seen active efforts to protect the use of computers and the international response to the problems of computer crimes, the same era saw the age of many of the protection of computer use or develop special about it texts as an amendment to the penal laws, and the same period has also seen a growing trend on the protection of computer programs legislation intellectual property, and affected by this trend and our Arab nineties witnessed the birth of a new copyright laws or modifying the existing laws to allow the provision of protection for computer programs [2]. Due to the special nature of the data the computer in terms of being non-material, and do what sparked the judicial application of the provisions of the criminal law on computer crime problems, and to ensure that perpetrators escaping justice for lack of laws or inability to snap to this novel crimes and safeguard the legitimate principle that no crime and no punishment without a legal text, and under the principle of measurement ban for criminal provisions of objectivity, for these reasons, but the face of the danger to the heavy losses caused by computer crimes, enacted many of the world private or criminal laws amended

penal codes have to ensure that the face of computer crime along the computer data from the data, information and programs. The main landmarks of the provisions of criminalization legislation introduced by comparison, and then we show the main parameters of the University for this Legislation to memorize the conduct of comparative law on computer crime [4].

## 2. LITERATURE REVIEW

In many countries there is mandatory legal legislation on the table in a special law (e.g. South Africa, France, Greece, Land and forgotten, Norway, Peru, Sweden), and in other countries can be found registered in another law, copyright law in (Australia, United States, Great Britain), and at the national Library in (Canada, Japan, Venezuela), or when the general libraries (Tasmania), in some cases, we find reflected in the legal basis (such as Chile, Cuba, Nigeria). The United States was among the first countries that felt the need for a separate legislation on crimes of his class at the federal level and state (ie at the state level) as both the US features a larger legislative package covering the computer and the Internet and telecommunications crimes issues. As in Europe, the eighties and nineties saw the age of computer crimes laws at the national level for the majority, if not all European countries, of course, along with the legislative collective effort as part of a united Europe, and the same period a legislative movement in this field in Australia, Canada and countries have seen from East Asia and America Latin [5].

We have emerged as a clear effort by national legislation in the comparative systems represent enact legislation to counter computer crime incident on the same financial value of the data or the so-called financial crimes related to the computer. This phase began mainly clear in the early eighties - even though it was launched in the seventies for the United States of America - and it with the development of the means of taking money banks and attacks on computer systems to destroy the foodstuffs, espionage and theft of data,

the developed countries and witnessed the birth of special legislation or an amendment to the penal laws to provide for these crimes after I realized that the traditional texts list does not criminalize non-actions, located on the physical movable, this in spite of the legislation is characterized able broad interpretation of the texts are contrary to the provisions of the laws of the Arab countries that confine Offences (generally) what happens on the physical money without moral (of course in money crimes) field does not contain phrases that help expand interpreted to include data computer (as with moral nature ).

These countries developed legislation in this regard in a row since 1975 in America and stretched over the eighties and nineties and were subject to modification and development in the light of the breadth of the activities of hackers at the end of the eighties and then the prevalence of the use of the Internet and created new styles and exploit their capabilities enforcement computer crimes and peek the internet led to the prevalence of unauthorized access and bypass security measures and spreading viruses and actions of disabled and denial of service and the destruction of e-mail content or altered, and actions stir up grudges and exposure to individuals' lives and reputations, and crimes of exploitation web sites in the acts of illegal content and illegal, such as promoting substances crimes porn and gambling. Generally in all countries where there is a legal system legislation published documents often called document libraries (books, magazines, newspapers, thumbnails, musical pieces, geographical maps, brochures, booklets, and other), which form the basis of the national group. And there is also a lot of countries where the documents audiovisual (audio recordings, films, videos and other) are also subject to the legal deposit (South Africa, Germany, Canada, Finland and France) and there are a few countries, including (South Africa, Canada, Denmark , Finland, France, Japan and Norway), which has allocated a place in the legislation for electronic Mencart, but keeps track of different ways [6].

As France and Japan, for example, have amended their legislation to the exclusion of online publications deliberately given the many technical problems posed by the acquired and maintained. To be sure, of course, that the national body in charge of the receipt of the documents to the law are often the national libraries An example of this (China, Estonia, France, Lithuania, United Kingdom) and the Library of Parliament may also be an example (the United States, Israel, Japan) And also the National Archives example of this (Antigua, Bahams, Senegal) or one of the large libraries official interests (such as Ghana, Hong Kong, Chad) or, rarely, a major university libraries (Kuwait, Liberia). The creation of a national set of documents published by the legislation in the broad sense must be based on a legal basis to ensure that the wishes of all publishers. In addition, and in order to take seriously by depositors must be available on the implementation, however, it is recommended, and the involvement of publishers in their preparation capacity and thus be in their interest to the immediate transmission of their publications to the national body ensures recorded and preserved for future generations [7].

### **3. Key Information Security Related Process**

Dealing with multiple information systems and processes in technology and communication processing and data exchange environment, but can generally identify the following main processes: -

- **Classification of information:-** It is an essential process to the construction of any system or in any activity related to the information environment and different classifications according to the facility throughout the search, for example, may be classified information to the information available, reliable, confidential and highly confidential or may be information available access and other prohibited reached and so on.

- **Documentation:** Information Operations require basically follow the written documentation system to document the system and all the means of exchange and processing components build. And is president of the documentation required and necessary for the system identification and authorization, and classification of information, and applied systems. As part of the security, the documentation required to be a strategy or security policy documented in writing and that the procedures and components be complete replaced document, in addition to dealing with the risks and incidents plans, responsible parties and their responsibilities and plans for recovery and crisis management and emergency plans associated with the system when danger occurs.

- **Administration and Personnel Responsibilities:** - The tasks callers information security system starts at the foundation of a good selection of qualified and depth of their theoretical knowledge and practical individuals, to be aware of the practical training requires constant training does not stop at the knowledge and experience they have appointed limits, and is president of the administrative tasks or regulatory consists of five elements or main groups: - risk analysis, policy development or strategy, develop a security plan, construction and technical security situation - hiring of equipment and means, and finally the implementation of plans and policies. It is important to recognize that the success of the administrative duties or collective property depends on the perception of all stakeholders in management (technical, administrative and financial duties) strategy and plan and duties of the security and the commitment of the institution as security issues and one of the subjects that perceived by all, and can all deal with regards to their duties of between security elements. On a personal level, or the level of

users, the enterprise can put adequate guidance to ensure public awareness and accurate security issues, but is required to build a culture of security among workers, which are divided between the obligation to comply with the ethics of the use of technology and the required procedures of all the Note any defect, and the institution that sets users what they need to do and more importantly what they are forbidden to do in the gallery using various technical means.

- **Means of identification and authentication of users and limits the powers of Use Identification and Authorization:** - The accessing computer systems, databases and information sites in general, it can be restricted in many ways to identify the personal user and determine the scope of use, which is known as the definition and Authorization Identification and Authorization systems. The definition or identity issue consists of two steps, the first way on the user's profile person, and the second to accept the way the definition or the so-called authentication of identity provided health. This characteristic means of definition varies depending on the technology used, the same means of access to information or the security services in the sectors of the use of systems or networks or segments of e-business and, in general, these methods are divided into three types: -

- Something that is owned by a person such as plastic card or otherwise.
- Something the person knows, such as passwords or code number or other personal
- Something linked to the same person or present therein, such as a fingerprint or iris, voice, and others.

The means of identification and authentication strongest, those means which combines all of these methods in a manner does not affect the definition of ease and efficiency at the same time. Whatever the method definition that is documented by the authentication system, they are

stand-alone and as will its use be subject to system security and guidelines security to be observed, Words password, for example, which is the most common of the other systems, requires that the subject deliberate policy in terms of length and components and to stay away from those words that are easy to guess or investigated as well as the subordination of use to the rules of non-informed and non-disclosure and preservation. When used means of defining appropriate to allow access to the system, and when authentication and matching process achieved and confirm identification (ID), the phase that follows is to determine the scope of use Authorization which is known Balkhuyl or authorization to use the information in the system sector, and this issue relates Login or control access to the information or parts control system Access control system [8].

- **Logging Performance Record:** - Contain different types of computers rather than the records that reveal the uses of the device and its software and access to him, which is what is known as performance records or access records to the system, the performance records of exceptional importance to take in the event of multiple users, specifically in the case of computer networks that uses components of more than one person, and in this particular case, any user networks, there is more than one type of performance records and documentation of use, and the performance records vary in kind and nature and purpose, there is a historical performance records and temporary records, and records of the exchange and system logs and records of security and records databases and applications and maintenance records or what is known as technical matters and other records. In general, the performance records mandated to determine who the user and usage time, and place, and the nature of use (content) and any other additional information depending on the activity itself [9].

- **Conservation operations Back-up:** - Operations of conservation related to the work an additional copy of the material stored on a storage media, both within the system or outside, and are subject to conservation operations to the rules have to be pre-defined and documented in writing and being committed to ensure the unification of conservation standards and protect the backups. The conservation time, and copy protection reserve, and the numbering system and the tab, and the mechanism of recovery and use, and location of conservation and safe, encrypted copies that contain private and confidential data, key issues must take clear and specific standards on them.
- **Security means the technical and intrusion prevention system:** - Multiple security means technical used in computers and the Internet environment, as multiple purposes and ranges of use, we have dealt with in the foregoing definition and documentation issues, specifically passwords and other means of identification. And take firewalls, in addition to encryption cryptography, as well as access control and detect Intrusion Detection System Systems (IDS), and systems and software viruses resistant increasingly important, but they all do not represent the means of security used, but is in addition to the means of identification and advanced documentation refer to them represent the most important means of technical security at the present time, and we'll show to these means to the extent available with the most important statement of its issues through the Security evidence internationally accredited and some of the norms and standards prevailing on them [10].
- **Dealing with incidents Incident Handling System:** - Regardless of the size and the technology used for security, and security standards and procedures in place, it is essential to provide an integrated system for

dealing with risks and accidents, assaults, and merely a requirement for the president to businesses, as in the case of banks and financial institutions. The first thing to be aware in this regard to dealing with accidents process, not just a project or a single step, in the sense that it integrated process related to the ongoing performance of graded subject to predetermined and followed carefully and discipline to the rules, and when what has been dealing with incidents on it's just a case arise when the accident we were in front case of failure represents a stand-alone elements of weakness in the security system [11]. The different components and phases and steps to deal with incidents from one institution to another depending on many factors related to the nature of the dangers shown by the risk analysis process and demonstrated established security strategy in the enterprise, and depending on the system of the protected and whether we are talking about a closed computer systems or open or databases or networks System or a combination thereof, and whether we are talking about an ad hoc service system or for services to the public over the network private or international, and depending on the function of the application replaces protection, as it varies steps, content and elements of dealing with incidents at Internet banks, for example, by the information site plans, however, and in general , the incident handling system typically consists of six stages (step by step) are:-

- Advance preparation and investigation and observation of containment and eradication, recovery and return to normal, and follow-up.
- Are the risks, threats and vulnerabilities and the types of attacks and assaults technology and methods

#### 4. Attacks and Risks Related to the Operations of Protection

If we want to we describe the risks related to operations of the same protection may be in fact in

front of all of the risks and attacks and assaults types, but it is a narrow technical standpoint, referred to the five types of styles within this community, some connection with the attacks that target system or entry strategy, some targeting system entering and processing data, some of which is classified as a verb first to achieve unauthorized access to various types of network operations, and we will refer briefly to these tactics and attacks, with the clarification of other names of activities, methods and attacks related to breach networks specifically, and a statement of the main weaknesses, according to the findings of the evidence specialized information security as a result of research studies [12]: -

- **Tampering (fraud) data Diddling:** - The targets of this attack or assault change data or create fake data in the input stages or extraction, and are in fact dozens of patterns and techniques, intercourse with her surveyor security and protection of data entry stage or extract.
- **Internet Protocol IP Spoofing deceive (stealthy exploiting transport protocols):** - The truth is that Spoofing the term does not mean invisible, is the term relation to fraud and deception, decoys, mock imitation, simulation and ridicule, but its use is now commonly regard to attacks viruses online, the idea here close to the idea of stealth, which offered her above when someone or take impersonating another user authorized to use, but the difference here, we are talking about a way purely technical, so the attacker through this method of rigging the address supplied with the transmitted data packet so that it appears to the system - of course, adopted in the exchange of data transport protocols and the most important here IP core - as a true sender from within the network, so that the system for data package to pass as a legitimate package allows title.
- **Sniff passwords (collected and captured) Sniffing:** - If the assault carried out by using passwords were often done in the past by

guessing passwords taking advantage of the weakness of general words and the prevalence of selecting individuals for easy words related to the surroundings of family or around work or their personal life activities, the new use of software that can sniff or capture passwords through touring in the part of the network or one of its elements and its monitoring of the movement of communication on the network, so this program in terms of the original collection of the first 128 bytes or more - for example - from all connect to the network being monitored and track movement contact them, and when the user prints a password or user name, the program (cantaloupe) collects this information and to copy them in addition to the types of these programs collect partial information and re-analyzed and linked together, as are some of them hiding capture activities after carrying out its mission.

- **Scanning and copying Scanning:** - a technique which uses a program (ware dialer or demon dialer processes), which is the likelihood of the program is based on the idea of changing the composition or switching possibilities of information, specifically about the prospects password or uses the phone number of the modem or so, and the simplest pattern which when used in the list of possibilities to change the phone number scans the list of large numbers arrived, including one that uses a modem to connect to the Internet, or a survey many possibilities for the password to connect to the correct word, which enables a hacker to access the system, and again, this is the style of a technical support mode technology is the program (scanner) rather than relying on human guesswork.
- **Attacks Exploit Additional Benefits Excess Privileges:** - The idea here relate to one of the most important protection strategies, the basic principle is that the system user - specifically within the organization - specifically his scope of use and the scope of authority for the system, but what happens in practice that the

benefits of use being increased without a risk assessment that or without the knowledge of the same person he enjoys the benefits exceed its competence and desires, in this case, any infiltrated the system will not only be able to destroy or manipulate the user who entered the system data through participation or by entering its own point, he simply will be able to various destruction even non-system files related to the entrance, which came from him because he invested the extra benefits enjoyed by the user who is entering through the entrance. The clearest example of this danger in the physical world, enabling people from entering the hotel room, for example, the Director of the purpose of stealing and finds in his room keys all safety deposit box or Master which opens the hotel rooms are all key. This alone gives us a perception of the importance of information security strategy in the facility Defining the privileges and powers may prevent the truth from the get of mass destruction and make breakthroughs irrelevant effect, and will not strategic conscious of saying that allow the user Doe has the advantages do not know about, but will not allow its existence to begin with.

## 5. Recent Trends in Cyber Crimes Protection

Along with major legislative efforts in this field, in particular, we saw the eighties and nineties and still activity growing in this field - the age of new rules and laws in the field of computers and the Internet crimes criminal proceedings, as these years have seen a wave of age on the protection of means and standard information security rules. It can memorize the modern trends of the protection of information technology crimes, including the following [13]:-

- Adoption of the new procedural rules in criminal assets field governing the inspection of computer systems operations and rules of prosecution and seizure and prosecution and investigation, as well as the adoption of a number of rules that protect the privacy as take

criminal proceedings in the field of technical offenses, and what might be called the guarantees of the accused informational.

- Growing legislation governing the provision of online services and standard specifications (standards and rules to protect the user).
- The growth of legislation in the field of protection of children and minorities from the dangers of the Internet (protection from harmful content).
- Growing legislative movement to protect against the risk of seizure of financial card numbers as well as the development of rules of protection of civil and criminal financial cards and electronic funds transfers.
- Develop a fundamentalist rules for the management of electronic publishing sites and responsibility for what is contained in it.
- Formation of rapid intervention teams on incidents and attacks on the internet and on the software and in the eavesdropping industrial espionage field.
- Develop encryption strategies and examine their suitability with the freedom of the flow of data (information security standards).
- Adoption of the security and legal strategies in the field of electronic commerce and related rights of contractors through communication and internet networks.
- Conclude international agreements on bilateral and competence in the field of technical offenses.
- Adoption of the legislation on the protection of industrial and technical protection of information security and protection systems of the activities of crime organizations in the gambling networks, money laundering, drug trafficking and prostitution field, regional and international measures and national security strategies.
- Development of standard specifications for computing and communication services and the Internet.

The first trace of the provisions of the legislation or the provisions of the amended laws to the laws

of sanctions and for addressing the phenomenon of computer crime, shows us the following facts:-

- **First:** this legislation varies in the identification of new criminal patterns and text on the criminalization and punishment, but as a whole does not depart from the minimum of these crimes that we have pointed out in reviewing the efforts of international organizations and regional scale.
- **Second:** The texts which involved the comparison of legislation on computer crime determines replaced assault with data computer technical broad either act was committed directly or used to facilitate the commission of another act, and the basis of criminality assault on the data does not describe an act that is easy to use a computer, or more accurately, data computer for committing.
- **Third:** many of the comparative legal systems tended to add new pictures of criminalization provisions of the section of the penal laws in their legal systems, and in that approving the application of the general provisions on the one hand, and the preference for automatic inclusion of these crimes to the Penal Code, rather than members of the special laws on the one hand again, we find this behavior has adopted the recommendations of the sixth Congress of the Egyptian Society of Criminal Law of which we have previously. But this is not a trend but tended Unitary many countries to members of the special laws governing the computer and internet crime issues, as in American law and British law and others, where he devoted a special computer-crime laws.
- **Fourth:** that the sanctions established by these laws, gathered mostly between anti penalties for freedom and financial sanctions for their impact combined in the face of the risks and losses of these crimes, and that certain laws, as France example, the text of the supplementary sanctions is to confiscate the devices used in the crime, and this course good for impact Profile (in the psyche of the actor) and

objective in the face of the effectiveness of this type of crime.

- **Fifth:** the technical wording of the texts of criminality in comparing laws on computer crime show, taking into account the technical aspects (reaching the system, stay in the system penetration, erasure and modification, automated processing, etc.), as stray wording in terms of the use of legal terminology function on crimes from the traditional terminology - for the most part. The user of the traditional terminology (such as fraud, or fraud, or destruction, or seizure, or theft the crime of theft of computer time only) take connotations differs in many respects from traditional meanings.

This highlights the main features of the legislation to protect the use of computers in comparative law and joints will show us the sights when analytical study of American and European trials next.

#### **6. Legislation and Legal Deposit**

Legal legislation, clearly in the public interest and national, where he ensures the acquisition, recording, preservation, and access to the publications of the national heritage and information. And information security, which is without doubt the main wing of the national cultural policy and should also be considered as the basis of national policy in the importance of the legislation for the development and promotion of a knowledge society in the Arab region and describes the development of cyber legislation in this area and the challenges facing the development and access to information.

The law is the result of all the legislation that is available on an executive's ability and governing the relationship between natural persons (private law) and those related to the state with a non-natural persons (common law) and those of states with one another (public international law). Laws aimed at regulating the political and social life of the community in order to ensure an orderly evolution of the Constitution as well as the fundamental law of the State where he shows that the main exporters to the law are made up of the

legislation approved by the National Authority and diligence body of legislative texts. Code of Justice decisions in particular those relating to the Courts of Appeal serving judges for the chapter in subsequent issues and at the same Roman rights of countries, there is the law governing the civil law, intellectual property law, labor law..... etc., these laws are the main source of legislation in that same year the legislation states, the judge has to rely on the base the previous law, which is associated to decide [14].

It is clear that the law is a form of written legislation that formally expresses E. Rada State about a particular issue, such as the legal system of the legislation. As the core his property lies in the executive ability that allows the state to use the power conferred upon it by the Constitution to force members of the community of natural persons or legal compliance. From here is the legislation concerning the Laws of information and knowledge cyber essential component necessary for the development of the information society regulatory and legal components of the environment as an important element for the provision of electronic trust services and insurance protection for users of cyber space and the aim of promoting knowledge-based society in Saudi Arabia.

On other side, Legal Deposit is the obligation imposed by law on any personal or moral nature of a lucrative goal or produces a public document preparation of any kind in order to deposit one copy or multiple copies of the designated national authority. It must be emphasized that the legislation on legal deposit covers all sorts of published documents, which often produce numbers and placed at the disposal of the public, whatever the means of distribution of all archive documents of official or private issued by natural or legal persons is usually summed up in pieces and single is not placed at the disposal of the public and are of a special nature or PC.

It should be remembered that the situation at the disposal of the public may mean the display or advertising and Embed. For example, a radio or

television program is published in the concept of legal deposit when it is distributed. As for Almcart electronic should be noted that any file in a single copy is a stored database in a distributor may be subject to legal deposit it at the disposal of the public means of technology that allows for the latter read it listen to it or watch it. Finally, the legislation is well prepared regarding the legal guarantees ordinary legislation or researchers to readers as well as abroad easy access of the national production of documents published thanks to the group established for this purpose.

### **7. Importance of Electronic Legislation for Knowledge Society**

With the development of the digital age and the growing efforts to build knowledge of modern society emerged the need to develop the electronic legislation (cyber) deal with the legal issues arising from the use of information and communication and its various applications in the economic and social life, technology has become the technology used in scientific applications in e-business and government services and in the interactions different between individuals and institutions in order to legitimize electronic trading on the one hand and the statement of its controls and limitations and to protect the customers of the other hand on this cyberspace (cyber) has made many countries to issue private electronic transactions and commerce laws [15].

As we know that it include e-government and e-commerce applications as well as e-health important data, some private individuals or institutions and this data may be sensitive or personal. The inclusion of issues relating to such data, which is stored in the computer systems of the privacy issues and data of a personal nature and in order of the sensitive nature of the protection of this data it was necessary to establish laws for the protection of personal information as well as the protection of all information that have the status of privacy and mutual either by mail or through other social applications by forbidding

middlemen from the use of this information without the owner's permission or misuse or placed inappropriately. On the other hand, and as a result of the growth of applications and mechanisms of social interaction and the entry of individuals in various social and cultural categories to use this cyberspace misuse and offending cyberspace it has grown some and took advantage of this space to the theft of financial or moral value information. Some also use it to infringe on young people or children have been the last few years has seen many of the crimes that have been implemented over cyberspace. In order to prevent the misuse of cyberspace it was necessary to criminalize harmful acts that take place across cyberspace and be considered like any other crime and embarked on many countries passed laws cyber crime deterrent bad and criminal practices and a tool for the prosecution of perpetrators of crimes and ensure beneficiaries' rights. In addition is the intellectual creativity in the field of programs and applications of information and communication technology of the most important hubs of creativity in the present day, which should protect these intellectual works, like the rest of the scientific and literary creations. And it was necessary to expand the protection of intellectual property laws to include software and databases, as well as electronic publishing

The building user confidence and consecration of security for all the parties involved in the use of information and communication technology is one of the necessary measures to ensure the growth and development of the information society enabling environment components. And it contributes to the availability of electronic legislation (cyber) in securing this environment also contributes to the improvement of e-commerce between the countries in the region and at the global level, especially with the approach of regional and international companies to rely on cyberspace as an essential tool for doing business exchanges and business and marketing. Thus, the availability of cyber legislation also helps to stimulate domestic investment and attract foreign

investment to develop the use of information and communications and the various applications of social and economic technology.

### **8. Threads cyber legislation**

Covering the electronic legislation (cyber) multiple threads are classified according to four types:-

- The first type includes the laws designed to protect human rights when the use of cyberspace (cyber) such as a personal nature and privacy data protection.
- The second type is criminal law, a special treatment of crimes and bad use of cyberspace (cyber).
- The third type is linked to the protection of intellectual property rights of software products and information and content exist on Internet.
- The fourth type in order to regulate the business of cyberspace.

We may need different types of treatment and classifying laws according to the following: electronic communications and freedom of expression and processing of personal data and cyber-crime, electronic transactions and electronic signature and e-commerce, consumer protection and intellectual property in the informational field and cyber security [13-15].

### **9. CONCLUSION**

The principles that should ensure respect for the right to privacy are the same as those already principles that are part of the sanctity of private communications and the protection of journalistic sources of human rights standards. There are fears that governments, under the guise of privacy protection, trying to limit public information, which are essential to the transparency of public services substrate. Governments should implement concrete actions to respect the privacy of Internet users, in order to avoid the censorship business. In this regard, it should create special laws to protect the privacy of individuals. Among the responses, it was also possible to determine the important privacy protection elements, such

as: the neutrality of the Internet, companies are treated and used for data of individuals when they arrive at the institutional applications and services. It is possible to contribute to the ethical principles that are based on human rights and to expand participation and the ability of everyone to access the Internet; and primarily through education and the promotion of those principles in society in general, on all levels of education. Specifically, these principles should form part of the international principles for freedom of expression, in order to ensure the largest possible amount of free access to information and knowledge. With respect to the uses and new applications and processes for research and analysis of the proposed establishment of observatories to monitor the research that can provide reports on the basis of the findings of investigations of the results; and with regard to the options available to interested parties for uses and new applications of information and knowledge, which is is key to promoting employment moral of the Internet. It is also proposed to conduct studies on technology convergence in order to develop strategies to support comprehensive access to the Internet. It is essential for young people in particular, that are monitoring any content highlights further research and strategies for this segment of the population, which has already emerged in the digital age.

### **REFERENCES**

1. Hulisi Ogut, Nirup Menon and Srinivasan Raghunathan (2005), "Cyber Insurance and IT Security Investment: Impact of Interdependent Risk", in Fourth Workshop on the Economics of Information Security
2. P Swire (2003), "Efficient Confidentiality for Privacy, Security , and Confidential Business Information", Brookings-Wharton Papers on Financial Services
3. Tom Lookabaugh and Doug Sicker (2006), "Security and Lock-In: The Case of the U.S. Cable Industry", Workshop on the Economics of Information Security (2003)

4. Rainer Böhm and Thorsten Holz, The Effect of Stock Spam on Financial Markets, Workshop on the Economics of Information Security
5. James Aspnes, Kevin Chang, Aleksandr Yampolskiy (2005), "Inoculation strategies for victims of viruses and the sum-of-squares partition problem", 16th ACM-SIAM Symposium on Discrete Algorithms
6. Benjamin Edelman (2006), "Adverse Selection in Online 'Trust' Certificates", Fifth Workshop on the Economics of Information Security
7. Hwankoo Kim, Bongjoo Park, JaeCheol Ha, Byoungcheon Lee, DongGook Park (2005), "New Key Management Systems for Multilevel Security", O. Gervasi et al. (Eds.): ICCSA
8. Sung Ki Kim, Byoung Joon Min, Jin Chul Jung, and Seung Hwan Yoo (2005), "Cooperative Security Management Enhancing Survivability Against DDoS Attacks", O. Gervasi et al. (Eds.): ICCSA 2005, LNCS 3481
9. Gu-Beom Jeong and Guk-Boh Kim (2005), "A Framework for Security Assurance in Component Based Development" , O. Gervasi et al. (Eds.): ICCSA 2005, LNCS 3481
10. Hyang-Chang Choi, Yong-Hoon Yi, Jae-Hyun Seo, Bong-Nam Noh, and Hyung-Hyo Lee (2005), "A Privacy Protection Model in ID Management Using Access Control", O. Gervasi et al. (Eds.): ICCSA 2005, LNCS 3481
11. Aghili, Shaun. (2010) Organizational risk management: successful achievement of business objectives hinges on the organization's ability to manage risk effectively
12. Lottering F, Dick A. (2012). Integrating knowledge seeking into knowledge management models and frameworks
13. Heisig, P. (2009) Harmonisation of knowledge management: Comparing 160 KM frameworks around the globe, Journal of Knowledge Management, vol. 13, no. 4, pp.4-3
14. Evans M, Dalkir K and Bidian C. (2014). "A Holistic View of the Knowledge Life Cycle: The Knowledge Management Cycle (KMC) Model" The Electronic Journal of Knowledge Management Volume 12 Issue 2 (pp85-97)
15. Choucri, N. (2007). The Politics of Knowledge Management. Massachusetts: Massachusetts Institute of Technology