© 2013,
Science-Line Publication
www.science-line.com

ISSN: 2322-4770
Journal of Educational and Management Studies
J. Educ. Manage. Stud., 3(4):394-400, 2013

JEMS

Comparative Analysis on Cyber-Crimes

Yousef Najafi[1], Azam Inanloo*[2], Sakineh Radmehr[3] and Zinat Jahani[4]

[1.] A Member of Academic Fellowship in Teachers Training University, Tehran, Iran
[2.] Islamic Azad University, Rudehen Branch, Rudehen, Iran
[3.] Tehran University, Tehran, Iran
[4]. Islamic Azad University, Islamshahr Branch, Islamshahr, Iran

* Corresponding author's Email: inanloo.azam@yahoo.com

ABSTRACT: So far legislators from several countries have purposed many definitions for cyber- crime but they have not yet achieved international consensus over this definition. This is due to several factors out of which those paramount ones are user's different level and exploitation from Information Technology in several countries. On the other hand, difference in criminal law system within various countries may serve as further reason and it causes on the other hand different reactions from several legal systems arises against a novel phenomenon. Overall, cyber-crime is unallowed use of cybernetic technology in order to access private sensitive information as well as confidential information from organizations. Basically, the extent of impact of those crimes which are committed in cyberspace is wider than traditional crimes and they will create more damages as well to the great extent. By casting a comparative and interdisciplinary glance at the newly approved concerning to cyber- crimes, this brief essay tries to purpose an eclectic definition from cyber crimes based on the aforesaid attitudes and remove some theme- and content – related ambiguities in this regard and imply briefly about types of cyber-crimes and classification of the content- related crimes in cyberspace.

Key words: Computer-related Crimes, Criminalization, Information and Communication Technology (ICT), Criminal Content- Cyber Crimes, Cyberspace, Content- related Crime

Review ARTICLE
Received 25 Jun. 2013
Accepted 20 Oct. 2013

INTRODUCTION

Approval of criminal laws and regulations is considered as a requisite for creation of security and facilitates development conditions in technological field while ICT is also not exception to this rule. But to codify an appropriate law which determines rights and tasks for practitioners in this area, creation of a common language among lawyers and ICT experts and legislator's attitude toward different issues is an undeniable necessity from its experts and users' point of view. Despite of all of its capabilities, IT is extremely vulnerable against threats since it has prepared the ground for committing of criminal actions, which have not been so far possible. Informatics Community's vulnerability to date due to cyber-crime has not been yet analyzed. On one hand, these crimes may include criminal activities with traditional nature such as theft, insult, and money laundering etc; and in the other hand, they comprise of completely modern crimes with new nature such as manipulation of data and damaging data. These newly- arisen crimes have managed to expose classic criminal law and its litigation procedure to a serious challenge. Some of their characteristics are way of their committing and enormous losses through using the least amount of sources with lowest cost, and lack of physical presence of wrongdoer in place of crime. Absence of a descriptive- analytical research about this subject and its importance tended the author to purpose information about anti- computer crimes rather than theoretical discussion about this matter and by means of it. As a result, we have tried in this article to study on nature, definition, and types of cyber-crimes and strategies of legal systems against them. The studies show that cyber-crimes have been gradually started their activities but it was accelerated along with an incremental trend. By 1970s, number of cyber abuses was so little that countries preferred to tackle with these crimes within the framework of traditional laws. Review of the cyber-crimes related rules and case law in Developed Countries suggests that in 1970s, these nations have initially reacted to cyber-crimes (crimes against individual rights) and then they started to exert change and reform in the regulation concerning to economic crimes and afterwards the crimes against copyrights. Ever- increasing growth in cyber-crimes after introducing Personal Computers (PCs) and particularly computer international networks not only increased crimes against privacy, economy, and copyrights (intellectual ownership), but also it has provided the possibility for attacking against other law- protected goals and interests. Crimes like production, presentation, distribution, and storing types of spam and racist content from computer systems and networks are considered as cyber-crimes (Sieber Ulrich; 1997). At present, many attitudes regarding cyber-crime are taken toward illegal transfer of capitals by electronic devices, cyber vandalism, viruses, and worms as well as documents counterfeit via computer. By 1970s, the subjects relating to cyber abuse have comprised of not only the crimes

regarding data protection but also computer- related economic crimes which are addressed as the main axis and area for cyber-crime this day. In this regard, the major crimes include computer abuses, cyber vandalism (sabotage), cyber exhortation, penetration, espionage, software theft, and other forms of products theft (ibid).

Definition of Cyber Crime

Since presentation of a standard definition from cyber-crime may be effective and useful educationally in training and awareness of minds and without a certain definition from cyber-crime, IT users and law enforcement authorities, including officials for prosecution, investigation, and court prosecutors, may be faced with uncertain and ambiguous condition and they may fail to fulfill appropriately their legal tasks and duties so purposing a definition from cyber-crime is important. So by presentation of a certain definition it is possible for them to establish international effective cooperation for campaign against cyber-crimes.

Measures taken by international organizations to define cyber crimes

The first effort was made for definition of cyber-crime by Organization of Economic Cooperation and Development (OECD) but expert group in this organization defined cyber abuse instead of cyber-crime in 1983 as follows. Cyber abuse is any illegal, immoral or unhallowed behavior relating to automatic processing and data transfer (Informatics Newsletter, 1994). Today, it is internationally and unanimously agreed in that cyber-crime should be defined extensively (Sieber Ulrich, 1997). Cyber Crime Expert Committee of European Council presented a manual and report in 198. It is called R (89) but does not purpose any definition from cyber-crime and it determined guidelines based on vote of member states. In this manual (guideline) term IT crime is purposed instead of term of cyber-crime where these crimes might be committed by a computer system. To define the given crime, the experts in this committee could not present an accurate criterion for cyber-crime so that thereby to determine examples of cyber-crimes (Legal Studies Development Center, 2005). UN interprets cyber-crime including criminal activities with traditional nature such as theft and counterfeit or with modern nature i.e. new ways for abuse. On time and intact assertion made by UN based on which some phrases like cyber-crime should be used not cyber abuse, is one of the most important issues (UN International Journal of Criminal Policy, Cyber Crimes Manual: 21/1). Cyber Crime Convention is an international document that its subject is cyber-crime. This convention was approved in an international conference with the presence of 24 members states from European Council (EC) plus four countries i.e. US, Japan, Canada, and South Africa in Budapest in 2001. Cyber-crime has not been also defined in this convention but some further examples were mentioned under title of cyber-crime and member states were asked to take measures against their criminalization by means of criminal laws. Term cyber-crime has been used in this convention and computer related crime is one of five groups of crimes that have been called under title of cyber (Legal Studies Development Center; 2003).

Cyber Crime definition from legal systems view in different countries

Since there is no fixed definition from cyber-crime that has been unanimously agreed so at present each of US states has the specific law that they especially addressing those crimes, which required the presence of computer (Jafarpoor, 1993). According to some of American lawyers' view, cyber-crime concept requires criminal behavior against computer in three forms and it is subjected to crime like information theft or hacking computer services and sometimes computer serves as device for committing crime like cyber fraud, cyber counterfeit, and child spam and also often means or end is not directly crime but they are placed through a criminal behavior along with another crime such as storage of child spam and unhallowed information storage that has been acquired via computer or another source. In other words, it is possible to enter another action in a criminal scene after achieving a criminal result (Legal Studies Development Center, 2003). According to definition made by US Ministry of Justice, cyber-crime is any illegal action which it's committing requires legal persecution or summons due to exploitation from cyber technological knowledge (Parvizi; 2003). Based on definition by Canadian lawyers, cyber-crime is any kind of criminal action including copying, use, shift, and access consideration or abuse from computer systems, cyber performance, and computer data or programs (Sharifi, 2003). Following to other attitudes from other countries like Germany, in Austria definition and interpretation of cyber-crime concept is any type of criminal action that computer is a device or way for committing them (ibid). French lawyers' view is unanimously agreed in that informatics crime, which is generally equivalent to cyber-crime and computer- related crime in Anglo-Saxon system, might include very different actions. This concept is not a legal description but it should be considered as a criminal subject. The given concept is so inaccurate and ambiguous that it could not apply to criminal law

as a class of crimes. Moreover, Crime Legality Principle in French law serves as a barrier that we could interpret criminal title in French law with this level of ambiguity.

French lawyers' procedure is in that they try to define interference domain of criminal law and determine what actions and to what extent to be considered as crimes and then they tend to comparison them with the existing law in order to fill the legal gap in this path for legislator. In French law, two analytical classifications were purposed for cyber-crime. 1- Crimes against persons (Damage to private freedoms and rights); 2- Crimes against properties and rimes against electronic equipment and data

In this classification, it is focused on consequence of actions not nature of action and criminal's motives, in fact. This classification may not include in many cases like actions against security of a country or economic system. Another classification, which show further characteristic of informatics (cyber) crime is:

1. The committed crimes that their subject is informatics (computer). This classification comprises those crimes that target computer like vandalism and information theft.

2. The crimes in which computer is the active or passive device for crime such as destruction or manipulation of data and cyber fraud.

In this classification also all criminal positions have not been considered since often computer may randomly prove opportunity for committing crime. According to the definition presented by some group of experts that has convened by the invitation of OECD organization in Paris in 1983: "The cyber-crime is any illegal, immoral, or un allowed action against automatic processing or data transfer." (Khoramabadi, 2007)

Classification of Cyber Crimes from International Organizations' View

Due to transnational characteristic of cyber-crimes, international organizations have made some efforts for classification of these crimes so that to create international consensus over identification of nature and campaigning strategies against these crimes by presentation of it to a country. In this chapter, we examine the measures, which have been made by international organizations regarding classification of cyber-crimes.

Organization of Economic Cooperation and Development (OECD)

Within a report, this organization has implied separately five types of actions that might be criminalized under title of cyber-crime.

Entering, manipulation, erasing or stopping computer data or programs that:

1- It has been done generally and with the intention of illegal transfer;

2- It has been generally done and with the intention of committing counterfeit;

3- It has been generally done and with the purpose of prevention from performance of computer and telecommunication system;

4- To violate the owner with exclusive rights for a protected computer program (copyright) with intention of commercial exploitation and introducing to market;

5- To access or overhear a computer or communication system intentionally without taking permission from the responsible officials and or by means of unfair goal

EC Classification

The purposed crimes in Manual R (89) by European Council (EC) are as follows:

I) the list that includes at least:

1- Cyber fraud

2- Cyber counterfeit

3- Damaging to computer data or programs

4- Cyber vandalism (sabotage)

5- Computer unhallowed access

6- Computer unhallowed overhearing

7- Unallowed reproduction of the protected computer program

8- Unallowed reproduction of a semiconductor

II) Crimes in arbitrary list are as follows:

1- Manipulation of computer data and programs

2- Cyber espionage

3- Computer unallowed use

4- Unallowed use of a computer protected program

Like OECD report, EC recommendations serve as a measure for introducing the actions with criminalization capacity under title of cyber-crime and in no way they are not considered as an effort for classification of cyber-crimes.

UN Classification

This organization purposed some of cyber-crimes as the joint and common crimes namely the crimes which their criminal nature has been accepted publically among countries- and some other actions that criminal nature has not been yet agreed by them but they have created certain problems for private and individual rights. From UN's view, joint and common types of cyber-crimes are as follows:

1- Cyber fraud

2- Cyber counterfeit

3- Creation of damage in computer data and program or their manipulation

4- Unallowed access to computer systems and services

5- Unallowed reproduction of the protected (copyright) computer programs (Parvizi; 2003: 24-32)

Convention classification of Cyber Crimes

Four classes of crimes which have been stipulated in this convention are the followings:

1- Crimes against privacy: Data totality and accessibility and computer systems

2- Computer- related crimes including counterfeit and fraud

3- Content- related crimes that include the following crimes:

3-1- To produce child spam with intention to publishing them in computer system

3-2- To present child spam via computer system

3-3- Distribution of child spam

3-4- Preparation of child spam

3-5- To put child spam at disposal with intention to publishing them in computer system

4- Crimes relation to violation to author's copyright and its relevant sites (Sieber Ulrich; 1997: 16)

Identifying and definition of content- related crimes

Given that content- related crimes, which are the products of illegal contents of data through cyberspace, preferred to other cyber-crimes in terms of variety and reproduction so majority of these crimes could not be committed in real time situation since these crimes out of which spamming is one of the outstanding example of them, are committed due to freedom to human innate interests within virtual environment of internet and computer and the reality of these crimes should be inevitably accepted. Content- related crimes are interrelated to freedom, vacancy, and human- animal desires so that they are monitored by public and social control and supervision so they are reflected further in cyberspace and IT industry. Content- related crimes are a new term, which has been formally and broadly entered into terminology of criminal law throughout world countries after approval in Convention of Cyberspace Crimes in Budapest on September 2001. Content-related crimes are the consequence of cybercriminal law, which has been covered by the nature of some committed crimes in real time environment, of course. Content- related crimes may be defined in particular and in general. In special definition, content- related crimes are those kinds of crimes that have been committed through illegal contents and against public decency and morality or physical or mental health of persons or intellectual personality. In this definition, material cornerstone of crime has been realized in cyberspace but its consequences have been identified in outside environment like insult and accusation against other one via computer system. In general concept, content- related crimes include some crimes in which content is end and means for committing crime- such as contents including computer virus- or the end (goal) serves as crime- like destruction or counterfeit of computer contents- or as an accurate term, content is neither means nor end for committing crime but it is converted into illegal nature and indicate its effect in outside environment. On the one hand, under this situation the illegal contents are not devices for committing crimes since through realization and fulfillment of these contents whether by formation or by publishing, presentation, or storing, crime is realized and in fact it is a means of affecting on society or the persons outside cyberspace; and on the other hand, illegal contents are not the goal (end) for criminal person since they are substantially value-less and illegal and thus unsupported and for this characteristic, no crime is committed against them. Here, target of crime is community or the person outside cyberspace. In any case, illegal contents are considered as crime per se and by their nature provided that they are subjected to some actions like production, publishing, storage or presentation etc and the presence of such contents on computer screen suggests committing such crimes. As a result, cyber-crimes are defined as their special concept in this paper. Content- related crimes mainly remind of sexual crimes or abuses or the crimes against public decency and morality (Judicial Studies Development Center, 2003).

Types of Content- related Crimes

Content- related crimes include visual, auditory, and written crimes in computer and internet system with the following examples:

1. Children and adult spamming

2. Spamming and destruction of identity

3. Defamation (including imputation of in chastity, accusation, insult)

4. Insulting to religious sanctities

5. Invitation or stimulation or encouragement or threatening children to commit crime

6. Training crimes or hazardous activities

7. Training hazardous or misleading thoughts and ideas

8. False statements of truth

9. Production and publishing abhorrent or racist contents

10. Threatening, annoyance, and bothering others

11. Sexual tourism

These crimes are committed under titles of illegal contents generally in written forms or through image or sound and they are common in one characteristic that is nature of illegality, worthlessness, and lack of ability to be exchanged among people since these contents which should be removed, may be corrected unless no legal and rational usage might be assumed for them (ibid).

Content- related crimes in Cyber Crimes Punishment Act

Fourth chapter of cyber-crimes punishment act- articles 15-19- concerns with content- related crimes so these items are implied in the following.

1- *Adult spamming*

According to article 15, "Anyone, who produces or publish pornographic contents by computer and telecommunication systems including female and male sexual organs or displaying sexual intercourse or action among human and human or with animal or transacts them in whatsoever, will be sentenced to from ninety and one days through one year imprisonment or payment of fine in cash from two million and five hundred thousand to ten million Rials or both of these punishments."

N.B. 1: If such contents of the above-mentioned subject are available for persons under age- 18 or they are published or presented for them the wrongdoers for this crime shall be sentenced maximally to either or both of the stipulated punishments.

N.B. 2: Production of false contents (including design and painting with intention for publishing or exchange of the included contents in regulations of this article)

In criminalization of the aforesaid cases for production, publishing, or exchange of spamming contents, defense from decency and morality in society is the major justification.

Material cornerstone of crime subject in this article comprises of the following elements:

1. *Criminal behavior* includes three actions: Production, publishing, and exchange of spamming contents within computer and internet system.

2. *Crime committing device*: crime as a subject of this article has been committed against public decency and morality of society and computer and telecommunication systems are means for production, publishing, and exchange of these contents.

3. *Crime committer*: Term anyone interprets all kinds of person including natural person or legal entity and if he/ she has played role in this crime, owner of images is not excluded from incurrence of the punishment in this article.

4. *Criminal consequence* of the crime is the subject of this absolute article and it is only sufficient to occur the action physical action with other conditions so approaching to criminal consequence is not considered as the condition for realization of crime since defamation of public decency upon committing crime is the subject of this assumed article.

5. *Mental Cornerstone*: General malice in intention for committing criminal actions is the subject of this article and due to absolute nature of crime, there is no specific malice.

6. *Punishment*: With respect to Article 640 of Islamic Punishment Law and perceived expedient conditions, the punishment is voluntarily stipulated for production, publishing, and exchange of spamming contents so that prosecutor may determine appropriate punishment for it by considering the amount of spamming contents and their qualities and background of committer.

2- *Crimes relating to persons under age 18*

According to Article 16: "Any person, who commits criminal actions by computer or telecommunication system, will be sentenced in the case of crimes mentioned as subject of Clause A, to one year imprisonment or payment of punitive fine in cash from ten million to thirty million Rials or both punishments and in the case of crimes implied in Clause B and C, to imprisonment from ninety one days to one year or payment of punishment fine up to two million Rials or both of these punishments."

A) Someone, who produces or presents or publishes or stores or prepares pornographic contents including display of genital organs or showing sexual intercourse or action by persons under age 18 and or make them available for others.

B) Anyone, who tries to promote, stimulate, encourage, invite, deceive, or threaten them to access persons under age- 18 to contents of subject in Clause A in this article or the previous article or to facilitates and or train them to access to the given contents.

C) Someone, who tries to train persons under age- 18 to commit crimes and sexual deviances or other crimes, suicide, or consuming psychotropic drugs and or invite or deceive them to promote, stimulate, threaten, or encourage for these crimes and or facilitate and or train them by committing or consuming them.

N.B. 1: Production and or storage or preparation of false contents will be excluded from this article if they are not used for presentation or publishing or making them available for others.

N.B. 2: Subject of the above article does not include that kind of contents, which are presented for

conventional scientific use or any other rational expedience.

Today, protection of children against risks of modern world, which its major part is realized in cyberspace, has been converted into an obvious subject for all countries. There is no legislation background to protect children against cyberspace in Iran but there is a history for legislation regarding protection from children versus pornographic and tedious images. According to provision 3 from article 3 of this law that concerns with way of punishment for those ones who committing unallowed activities in audio- visual items approved on 23/11/1993, employing children for storage, display, presentation, sale and reproduction of unallowed tapes as subject of this law, will lead to enforcement of the maximum stipulated punishments for the committer.

3. *Crimes relating to spamming and Personality destructive writing*

According to article 17 in this act: "Everyone that alters and or destructs and publishes other movie or picture or image of someone by computer or telecommunication system and publishes it by knowingly its destruction and alteration so that this action leads to defamation or damage and loss for that person, will be sentenced to imprisonment from ninety one days to six months imprisonment or payment of punitive fine in cash from two million and five hundred thousand to ten million Rials.

N. B.: Committing this crime against leader or heads of three major official bodies will be subjected to the maximum period of imprisonment or the stipulated cash fine in this article. This article was enacted because cyberspace has been converted into a suitable area for insult and spamming against personality of people.

4. *Publishing or availability of private secrets*

According to article 18: "Any person that publishes movie or image or picture or private or familial secrets of other person without his/ her consent or make them available for others by computer or telecommunication system in such a way that it leads to loss and damage or normally to disrepute him/ her, will be sentenced to ninety one days to six months imprisonment or payment of fine in cash up to two million five hundred thousand Rials."

Contents of crime in subject of this article are only valuable for their owners and they are publically worthless and on the other hand, criminal description of this article means publishing these contents and making them available as movie and or image and or private secrets of other people without their consent so that this tends to protect from privacy of persons.

5. *False statements of truth*

According to article, "Any one, who publishes false statements via computer or telecommunication system or makes them available for others or attributes to natural person or legal entity or official authorities some actions against truth basically or as quotation so that to cause confusing public opinion or official authorities or loss for third party, will be sentenced to from three months and one day to six months and payment of fine in cash from two million and five hundred thousand to ten million Rials rather than criminal rehabilitation."

N. B.: The crimes as subject of article 17 except for this article and articles 18 and 19 as well as excluding of publishing or making false statements of truth available or presentation of actions against reality which may lead to confusion of public opinion or official authorities, will not be prosecuted only by complaint from private plaintiff and it will be stopped by his/ her forgiving.

With some little changes, this article is the repetition of article 698 of Islamic Punishment Law where punishments are determined arbitrarily and crimes may be forgiven (Judicial Studies Development Center, 2005).

Different types of cyber-crimes are common in one point that is illegal exploitation from modern cyber technology and communication for committing criminal actions. As the modern technology purposes a strategy for tackling these crimes; on the other hand, criminals are benefitted from the state- of- art technologies for this purpose and they advance one step forward than security systems. So there is no more secured way of campaign than observance of precautionary measure; therefore, one should be careful for and look out anonymous emails, chat-rooms, flash memories, and suspicious websites etc.

CONCLUSION

With all possible basic and formative defects, approval of new law for cyber-crimes may serve as a positive stride toward campaign against criminals and contribution to ICT development. As it mentioned initially, it was intended to raise some questions about Cyber Crimes Law in reader's curious mind. In any case, it should be mentioned that it is possible for non- lawyers to seem boring these subject because legal texts are often complicated and of course Cyber Criminal Law is not also exception to this rule; however, it should not be forgotten that we are currently faced with a law that covers all computer and internet users throughout the country and most importantly, what is more important than the rights which have been attached for us in this law, including several tasks that are assigned to us. To make aware

of rights and tasks that this law has been determined for us, the easiest way may be reading of legal text and study on critics for this law, if necessary.

Basically, legislator's task is to cover unwritten norms and rules in the form of legal law and to support from community's values inter alia. To tackle with behaviors which might violate a certain value, legislator takes several strategies in order to protect from the given value. Enforcement of punishment and declaration of a behavior as crime that is called criminalization is one of these strategies.

Criminalization means law for doing or not doing a certain behavior and declaring it as forbidden and to determine sanction for any person who violates from this order. If these sanctions are coercive, they are called criminal sanction or punishment. But there is also other class of sanctions, which they are called non- criminal sanctions like guild, administrative, disciplinary, and moral sanctions etc. in a plan and non- professional expression, these two types of sanction differ from each other in costs that may incur for each of them. Since punishment is considered as a kind of severe and official reaction by the government against criminal person and it is followed by some negative consequences and a lot of costs both for criminal and society (e.g. costs for maintenance of criminal in prison or the problems which encountered for family of criminal person) so to date it is usually tried to use non- criminal sanctions- which are more constructive with lower cost than punishment, especially imprisonment. By study on Cyber Crimes Law we notice that there are only two forms of sanctions and punishments: cash fine and imprisonment. This may indicate that legislator has not taken a defendable rationale that is derived from essence of criminal law, characteristics of IT field, commercial requirements in national and international arenas, and conditions and expediencies of current society in justification of the reason for enacting of the enforced sanctions and even cases of criminalization (Firoozmanesh, 2008). The last point is that this question may be purposed that whether the ratified laws could provide duly the interests of natural persons and legal entities, who are related to ICT field, and even in some cases it also determines some legal barriers and restrictions against route of their activity or not. This is another subject which it is impossible to investigate it within this limited time.

REFERENCES

The review of IT legal aspects (2005). Judicial Studies Development Center, State Informatics Supreme Council, Qom: Salsabil Press.

Firoozmanesh, A. (2008). The essay on review of Cyber Crimes Law.

Khoramabadi, A. (2007). Cyber fraud from international perspective and Iranian status. Quarterly of Legal Journal from Tehran University faculty of Law & Political Sciences; year 37th, 2.

Parvizi, R. (2003). Cyber Crimes. Judicial Studies Development Center.

Sharifi, M. (2003). Cyber-crimes in criminal international law. MA thesis, Islamic Azad University (IAU) Tehran branch.

Ulrich, S. (1997). International appearance of Informatics Criminal Law, transl. by Deziani Mohammad Hassan, Manual of Cyber Crimes, 2 & 3, Secretariat of Informatics Supreme Council .