LEGISLATIVE REVIEW OF GENERAL AND SPECIFIC CRIMINAL LAW, CYBER CRIMES CRIMINAL LIABILITY, AND INTRUDING ON INDIVIDUAL PRIVACY IN CRIMINAL LAW

[a]ALI KASRAY KERMANSHAHI, [b]MEHDI SALIMI

[a]Department of law, International Branch, Islamic Azad University, Bandar Anzali, Iran
[b]Department of law, Qaemshahr Branch, Islamic Azad University, Qaem Shahr, Iran

Email: [a]Ali_Kasray@yahoo.com, [b]Mehdi.salimi.55@gmail.com

Abstract: The current paper investigated the terms of criminal liability in cases of cyberspace crimes. The reason for investigation of instances was that we found it tough to provide a definition of the crime since these crimes cover a wide range without a single issue and cannot be addressed in the context of a concept to define. Moreover, we examined legislative aspects of general and specific criminal law. Finally, it should be noted that the current paper mainly focuses on crimes against public morals and ethics occurring in cyberspace.

Keywords: Crime, Cyber space, Criminal liability, Ethics, Computer, General, Specific

1 Introduction

Legal rules evolve and progress as other sciences. Legal research contributes to the development of legislation by addressing those aspects of reality overlooked by legislators with a big share in amending legislation. It seems that the violation of morals and ethics concepts in cyber space is less taken into account and the legislator is required to address them. Some cyber crimes are more important than the others, because directly contribute to ethics and morals and face families with serious crisis. The current paper seeks to provide answers to the following questions:

1. Is there any criminal liability in cybercrimes?
2. Can we say cybercrime is affecting public morals?
3. What is the legislative approach in the legislation against these crimes?

Accordingly, we reviewed legislative of general and specific criminal law, cyber crimes criminal liability, and intruding on individual privacy in criminal law.

2 The concept of cyber crimes

There is no commonly agreed single definition of "cybercrime". The first organization to initiate cyber crimes definition was the Organization for Economic Co-operation and Development (OECD) through a group of experts gathered at the invitation of the organization in 1983 in Paris. They defined cybercrime as "Misuse of computers, including any illegal, unethical or unauthorized behavior of automatic processing and transmission of data."The misuse of computer is the cybercrime in the provided definition, although the definition does not explicitly refer to. Another definition of cyber crime reads: "Any positive illegal action uses computer as a tool or thread is a cybercrime". The above definition is not satisfactory and comprehensive because refers only to the material element of the crime and overlooks other elements of the crime as well as instances of cyber crime. Germany's Federal Criminal Police Office provided the definition of cybercrimes: "Computer crime encompasses all things, conditions and qualities in which forms of electronic data processing are used as the tools or target of committing a crime or as the basis for the suspicion that a crime has been committed". Also under the US Ministry of Justice "any act of violation of the penal code that requires knowledge of computer technology to commit the act, track or trial is a cyber crime".

3 The concept of liability and its variants

Dehkhoda dictionary defined the term as guarantee, responsibility, obligation, accountability and being aware of responsibility. Liability can be classified into two civil and criminal responsibilities, the civil liability discussion is out of the article scope and the current paper addresses the criminal liability. Lawyers have taken criminal liability in two different ways; one meaning constitutes "the liability to bear the criminal consequences" and the other "coercion to bear the criminal consequences". The former represents the abstract aspects of liability while the latter is the indicator of concrete aspects of the liability. Moreover, Imputed Liability is a kind of liability assumed as the liability of the person (whether natural or legal) without having all real terms of criminal liability ranging from spiritual to objective conditions alleged to be responsible. We discuss criminal liability in cyberspace, thus it requires articulating the challenges in cyberspace law and criminal liability.

Many legal scholars believe that the Cyber Crimes concept has created serious challenges to the traditional model of criminal law, so that the current criminal law is not capable to deal with problems that arise in cyberspace. In general, criminal law in principle is based on historical cultural and social community facts and shaped by certain social realities over the centuries. When, conflict arise over time criminal law is not be able to solve the problems (Kashian, et al., 2005). Basic features of cyberspace and cybercrime includes extensiveness, universality, hidden, the selectivity of information, lack of control, lack of vicinity of the perpetrator and the victim, the prevalence of crime and victimization, ease of crime, survival of criminal phenomenon, the extent of harm caused by crime, as well as detection, investigation and prosecution complexities. In fact, criminal law tries to apply preventive strategies with certainly less cost, more secure and more effective than persecution of the criminal instead of applying the traditional rules of law, due to the characteristics of cyberspace; and this is why non-criminal prevention methods are priorities. In the meantime, particular attention to technical solutions that unlike educational strategies are easier to receive binding nature without a long time required for institutionalization gain special importance. Clearly, this is also causing major developments in the area of liability, of course, the preventive measures task put some liability on others and the decentralization of liability of the main perpetrators makes others bear part of the liability.

The current paper has classified the contents into two sections, described the concepts and general discussion on the issues;

Cyber Crime General Criminal Law, Cyber Crime Specific Criminal Law

4. Cyber Crime General Criminal Law

4.1 Components of cyber crimes

4.1.1 Legal element

1. Production, reproduction, distribution and storage of unauthorized works

Legislator in Article 3 of the Law (2007) has shown specific approach with a harsh response to the factors involved in audiovisual works contrary to public morals and ethics (the spread of non-ethical).

4.1.2 Material element and the realization of forms of crime

Legislator in the above-mentioned Article (Article 3 paragraphs and notes) provides the realization of the different elements of the crime, the subject of this article.The form can be divided into 18 types in the study of the behavior of the material elements of the crime.The author tries to clarify the facts on different forms of crimes through the provided explanations in terms of the factors involved in crime and the type of material behavior given various punishment to each category that in some cases is two-fold as the cases may be explained below:

1 Distribution: distribute, disburse, divide

2 Proliferation: to add, multiply

3 Effect: signs, logos and symbols remaining from anything, remains of serious or practical work

4 Production: create, procreate

5 Rape: literally means contrary to tolerance, and the so-called criminal law action of forcing someone to do something without their consent, whether by action or material incentives, or not.

6 Reluctance: in criminal law is the impact outside force on the offender so that it is usually impossible to resist.

7 The key factors of production of audiovisual works: include producer (investor) director, camera person, cast the main roles

8 Wholesale: The number of more than copies of tape or CD

9 Vulgar: vulgar audiovisual refers to works that have scenes and forms and content against Islamic law and ethics to promote and conclude. (Note 1, Clause b of Article 3)

10 Publish: publishing vulgar audiovisual through electronic communication and computer or other similar means and techniques is an example of multiplication and dissemination.

11 Pornographic: pornographic audiovisual are those with female nudity or genitalia or sexual intercourse contents.

4.1.3 Mental element

The offenses set forth in article 3 of the Act of 2007 and according to enumerating the various types as a material element of the crime, all alternatives are essentially spiritual elements a deliberate crime and obtaining the malicious intent to commit is necessary.

Of course, in some cases, the legislator specifically identified examples of corruption on earth the accused is sentenced for the offense (corruption on earth) that the spiritual element of the crime of corruption on earth should adhere to the same principles that according to Article 183 of the Islamic Penal Code, in hodod, creating fear and deprivation of liberty and security of persons as criminal intent must be established.

4.1.4 Enforcement

Names Act 2007, after the study of the law, particularly Article 3 of this law clearly come to the conclusion that Law- makers hastily wrote enforcement of criminal laws associated with it, a kind of haste in legislation (substantive) and also in composition (form). An example may be the crime of "key factors of production". In an assumptions, they are not subject to as a corruptor on earth and the legislator has inadvertently forget a sanction for perpetrators of behavior while legislator has provided sentence to the secondary factors of production in Note 3, Clause (a), Article 3, but main factors that normally should be punished more severely than non-original elements have been overlooked. And another example of audiovisual "producer" less than 10 copies, that legislator has criminalized the act again, but inadvertently does not provide any penalty. In some special circumstances, the legislator intensifies some of the penalties.Note 3 Paragraph B of Article 3 reads:

[Use of minors for maintenance, display, supply, sale and proliferation of unauthorized tapes and compact discs under this Act, causes the maximum penalty prescribed for the agent].Therefore, pursuant to the above provisions, the use of minors in the cases mentioned above leads to the exercise of maximum punishment. It should be noted that tapes and compact discs shall be described as "illegal" or otherwise they are not subject to the provisions of this Note as maximum penalty prescribed.

Also note that there is no mention of offenses against the dignity of people in the Budapest Convention on Cybercrime, but Iranian legislator's attempt to criminalize such acts are properly is important. This category of cyber crimes includes three categories of offenses; first as defamation by publishing fake audio and video content, second, as people defamation by publishing the secrets of their private computer, and publishing lies, each with legal, material and spiritual component, which we will refrain from mentioning them due to limitations.

5 Cyber Crime Specific Criminal Law

First we discuss crimes against morality and ethics and then turn to cybercrime punishment.

5.1 Crimes against public morality and ethics:

According to the provisions of our law of Islam, crimes against public morals and ethics are not limited to the publication of images of people younger than 18 years and criminalized of all acts incompatible with chastity. For this purpose has taken into account three criminal cyber crimes against chastity and public morality. The first is production and distribution of contents contrary to public morals. Legal element of the crime is Article 14 of the Cyber Crime and its amendments. It provides: Everyone publishes, distributes or deals pornographic content by computer systems or telecommunications and data carriers, or produces or stores to trade or corrupt will be punished by Ninety-one days to two years imprisonment or a fine of five million Rials (5.000.000) to forty million Rials (40.000.000) or both.

The second is to provide grounds for facilitated access to the obscene or vulgar contents that is the legal element of the Article 15 Clause (a) of the Cyber Crimes Law that provides: Whoever organized by computer or telecommunications, and data carriers, committed the following acts, will be punished as follows:

(a) Whoever stimulates, encourages, threatens or bribes or tricks, facilitates access to or teaches people in order to achieve pornographic content is subject to imprisonment of ninety-one days to one year or a fine of five million Rials (5.000.000) to forty million Rials (40.000.000) or both. Committing acts of vulgar content results in a fine of two million Rials (2,000,000) to five million Rials (5,000,000).

The third is providing grounds for committing acts contrary to chastity or moral grounds through computer systems or telecommunications that is the legal element of the Article 15 Clause (b) of the Cyber Crimes Law that provides: Everyone committed the following acts through computer systems or telecommunications and data carriers will be punished as follows:

Whoever stimulates, encourages, threatens or bribes or tricks, facilitates access to or teaches people drug abuse, suicide or sexual relations is subject to imprisonment of ninety-one days to one year or a fine of five million Rials (5.000.000) to forty million Rials (20.000.000) or both.

5.2 Crimes against accuracy and integrity of data

Legislator in this category of computer crimes has predicted three general headings: computer forgery, destruction and disruption of data or computer systems and, theft and computer fraud. Computer forgery as is a crime against accuracy of data, destruction and disruption of data or computer systems is a crime against integrity of data and telecommunications systems. Theft and computer fraud also investigates the theft and cyber fraud (Qadir Golkarian et al., 2005).

At the end we briefly refer to the competence jurisdiction of the criminal courts on non cyber crimes, because determining the competent court either plays a major role either in the realm of domestic or transnational in scope, location and geographical borders. The discussion of cyber space shows the without border nature of the space regardless of geographical location and thus theories based on geography and borders on the non-cyber crime cannot govern issues of the crimes committed in its realm. Therefore it is necessary to provide theories and new rules in addition to the rules governing the jurisdiction of courts in the non-cyber crime problem to express rule to determine the competent court for crimes committed in cyber space.

However, it may be possible to observe some traditional theory despite the disparity of them with special features of cyber crimes as its non geographical borders nature. While others such theories, has little relation with the offense, may be fully applicable on cybercrime. However, the jurisdiction or actual support is created based on the outcome of the offense and the danger created for a particular country, and the location and method of committing plays no special rule in determining the competent court which is fully applicable on cybercrime. So, non cyberspaces theories have been proposed with other criteria expression and analysis in expressed theory in terms of crime competent jurisdiction in cybercrime.

6 Overview of cybercrime on social networks

The social networking technology is undeniable phenomenon with public welcome due to its ease of communication and many facilities. Misusing social networks especially Facebook, Instagram, and Telegram and. etc. are on the rise in line with the increasing use of cyberspace. The abuser usually intrudes on cyberspace by hacking sites or personal profiles or stealing personal information and or offering insults and threats or publishing personal photos and videos. Thus, given the novelty of computer crime, the prosecution of offenders and complain and track and prove of this crime requires detailed information on the law as well as that of the cyber domain. Common the social network crimes include:

a) Content against public morals and ethics
b) Content against security and public peace
c) Content against Islamic sanctities
d) content about cybercrime
e) Provocative content, promotes or inviting to criminal acts
f) Criminal content related to audiovisual and intellectual property
g) Criminal content related to presidential and parliamentary elections

More recently, Telegram cybercrime is also added to the list of examples of cyber crime, because this is a newly launched computer network. Telegram Social Network has opened a new place in Iran with a growing internet marketing crime rates in such a short time, and measures should be taken in this regard. Telegram penetrated in large among individuals, and thud along with the many opportunities in the social network, we discern abundant and sometimes irreversible threats, as well.

7 Conclusion

At the end, we conclude that identification of the crimes in cyberspace and pillars and principles of liability and the conditions for its perpetrators along with the legislation can contribute to the process of preventing and reducing cyberspace crime. Accordingly, the crimes occurred in cyberspace are formal and coordinated efforts to deal with a cybercrime will be complex and complicated if different countries judicial systems do not provide the same definition of cybercrimes. Moreover, domestic reactions and dealing with a cybercrime do not suffice, and International Coordination is essential in this regard. Regarding crime detection, Police and judicial authorities are required to gain full knowledge of computer in the investigation and judgment. It would involve providing the necessary technical facilities, trained investigators in the field of computer and issues related to data and information as well as regulate the procedure by cybercrime. The jurisdiction procedures should determine the investigating authorities and judges on how to achieve the information contained in a computer environment to detect and prosecute computer crimes and gather evidence. Also, to provide resources with the admissibility of evidence of arrest and trial of the perpetrators of such offenses so that to prevent intruding on individual's privacy and freedoms.

The most serious action that has been done in the realm of cybercrimes is the Fighting computer crime judiciary bill prepared in 2002 that the bill was not passed and ratified by General Assembly. However, legislation in 209 on the subject of the current treatise has already helped accelerate the pace of this process. Finally, in the current paper, we concluded on the policy of Iran regarding the cybercrime to prevent the criminal and non-criminal occurrence of the crimes by investigating elements of the material and psychological conditions of cybercrime and its penalties, as well.

Reference

1. Babazadeh, G.: *The European Convention on Cybercrime.* ASMT, 2003.
2. Khoramabadi, A.:, *the history, definition, and classification of computer crime*.
3. Dehkhoda, A.: *Persian dictionary*. Second edition, Tehran: Tehran University Press, Volume IX.
4. Razavi, Mohammad, *cybercrimes and the role of police in preventing and discovering of the crimes*, Police Knowledge Quarterly, Ninth Hall, 2007, No. 1.
5. Aalipoor, Hassan, *Content-related offenses: technological Black content*. 2007. p. 72
6. Cybercrime law enacted in 2009.
7. Kashian, A.: *Internet strategy*, the Secretariat of the Supreme Council of Information, Tehran, 2005. p. 283.