Indian Journal of Fundamental and Applied Life Sciences ISSN: 2231– 6345 (Online)
An Open Access, Online International Journal Available at www.cibtech.org/sp.ed/jls/2015/02/jls.htm
2015 Vol. 5 (S2), pp. 3248-3255/Behbodi and Naderi
Research Article

LEGISLATIVE CRIMINAL POLICY AND CRIMINAL PREVENTION OF CYBER CRIMES IN IRAN AND INTERNATIONAL DOCUMENTS

***Bahareh Behbodi and Somayeh Naderi**
Department of Criminal Law and Criminology in Islamic Azad University of Kermanshah, Science and Research Branch
**Author for Correspondence*

ABSTRACT
In this article Iran's criminal policy is introduced for introducing the position of new generation of communication crimes and information called cyber crimes. Criminology in the cyber environment is a necessity for today and tomorrow and introducing and legitimizing cyber environment is unique and unpredictable. The law of computer crimes approved in 26, May 2009 is a new law that caused a development in Iran's legal system and represents criminal support of new values in Iran's society. By approving this law some new concepts and crimes appeared in Iran's criminal law that each of them needs precise and expertly investigation. Most of the cyber crimes are old and classic crimes in criminal law, but beside technological development, their commitment underwent some changes that in this law are investigated as computer crimes. Of positive points in this law at first we can example criminology of the most of the criminal crimes and allocation of a chapter to intensify punishments. In the second stage also considerable criminal support in the law of computer crimes is for supporting real criminals of these crimes in which modesty, honesty, and entire essence of them whether mundane or spiritual will be endangered and damaged.

Keywords: *Cyber Crime, Computer, Virtual Place, Legislative Criminal Policy, Crime*

INTRODUCTION
Criminal policy is a field of study that according to data, scientific and philosophical findings such as criminology findings and based on historical conditions try to establish and provide suppressing and predictive educations that are applicable in relation to crime and criminal. Mark Ancel- the French Judge (1954) believes that criminal policy is both science and technology and its subject is preparing the best method of establishing common rules beside findings of criminology (NajafiAbrandAbadi, Ali Hosain and Hashem beige, Hamid, Criminalogy thesis, 2011)[1]. Based on offering the concept of cyber crimes it is necessary to specify this concept "cyber environment is a virtual and imperceptible environment in international network spaces that in this environment entire information about people's relationship, cultures and whatever exist on the land is sensible physically that exist in one digital space digitally that is accessible to users and using computer its components and international networks are correlated. Cyber environment is still in primary stages. Nature of these crimes and misusing in such new virtual world never observed in the real world. Insufficient security of technology along with virtual nature provides a good opportunity for criminal individuals (Bastani, Boromand, Computer and internet crimes, Behnami Publication, Tehran, 2004)[2].

As cyber space is a space for development and achieving at information, it is a very strong space for criminals to act what they intend. But for growth of this space governments try to offer an influential for campaigning against these crimes, and as cyber network has a cyber network it has a universal approach. Having a comprehensive law is in line with international society and it is a priority for every legislating act to be able to support information and users computer systems to control their problems. The most important cyber crimes such as: traditional crimes in digital environment (computer fraudulent, computer spy, breakout and publication of information through electronic post, illegal purification of money, smuggling drugs) and crimes related to the copy right and programs, crimes related to electronic commerce and future crime related to the cyber terrorism. As mentioned for newness of such crimes and inefficiency of legal crimes in computer crimes and having no sufficient experience to resist against many

modern cyber crimes and still there is no comprehensive studies under this title and such issue added necessity of authorship.

Theoretical Framework of the Research

In this section of the article we discuss review of the related literature about legislative criminal policies and preventing cyber crimes.

The Concept of Criminal Policy and Different Types

At first the concept of criminal policy should be analyzed and different type of them should be stated:

The criminal phenomenon in a developed meaning just do not benefits from criminal society that means violation, offense, and crime, but set of behaviors that are other than criminal law and corrupt social order and they are in the form of lack of acceptance and regulating social norms.

Criminal policies other than such behaviors and criminal behaviors try to propose responses formally and informally regulating the principles of human right, therefore, criminal policy is formed just in the form of one design and general strategy in the form of social policy of a country.

A. The concept of Strait (Lazoroj, Kreisten, criminal policy , p. 21)[3]: criminology and criminal punishment by government of government with criminals, the most important form of punishment with crime and criminal, for this reason the first applications of criminal policies is appointed in a meaning that is equal to something equivalent to criminal system that is based on crime-punishment and low ()[4].

B. Expanded concept: today criminal policy in entire tactics and preventive activities that are applied by government and civil society, separately or by each other's cooperation to prevent crime, campaigning against crime, modification or suppression of criminal".

Different types of criminal policy: every criminal policy, to have access to their purposes needs effective tools that based on the used tools we can divide them to legislative criminal policies, legal-criminal policy, applicable criminal policy and cooperative criminal policy that according to necessity of the subject only definition of legislative criminal policy is dealt with.

Legislative criminal policy using legal tools that involves constitution, criminal laws and …, tried to have access to purposes of criminal policies (Delmas Marti, Miri, Great systems of criminal policy, p. 15)[5] and a set of tactics for complaining against crime that is reflected in the law and benefits legal application guarantee. This type of criminal policy while having legal competence, that has criteria and principles of different types and represents dominant general principles on criminal system of society and sometimes relies on deviated actions or criminal actions and sometimes relies on personality of the individual and commitment of the criminal action, and also it is based on criminal personality respecting the view that timing law is based on criminal policy that "personalizing" criminal application, social control are for helping and preparing the return way for criminals and deviation to society. In this state it is possible to punish application guarantee that is definite and is not in line with committing crime, because what is important is personality of the criminal or deviated individual not committing action (Kristin Lazroj, p. 92-94)[6].

Definition of Cyber Crime

The term cyber crime has a direct relationship to cyber space. The first formal activity that clearly referred to the term cyber crime, activity of UN in November 1986 is based on formation of the committee of experts to fight against cyber crimes (Computer crime, reporting the achivements of UN in relation to advices 2010, (9) r, p. 132)[7].

The newest international document that the term cyber is referred to is convention of cyber crime and justifiers and approvers of convention of cyber crime without any description about the concept of cyber crime that accepted it as the name of convention. Cyber crimes convention's silence with respect to the meaning and concept of cyber crime and applying terms such as computer crimes and crimes related to the computer in this convention and justifying reports of them causes different understanding of the term cyber crimes in international documents.

Cyber crimes in domestic law are called crimes that are committed in non-physical environment against information technology. Crimes of cyber space in domestic laws attract our attention in different views: Classic crimes (traditional) with cyber description: currently wherever there is computer networks, the

tools of committing traditional crimes such as fraud, faking would be possible with cyber description. Crimes against secret data and computer and telecommunication systems: such as crimes that belong to this category, that it is possible to refer to illegal listening to telecommunication data in a personal relationship or data that are considered as the unit of value for domestic and foreign security. Of crimes that will be categorized in this set we can refer to illegal listening to telecommunication data in a personal relation or secret data that are considered as value unit for domestic and foreign security.

Crimes against accuracy and totality of data and computer and telecommunication systems: changing, creation, stopping computer data for fraudulent, misusing, destruction in data or electromagnetic waves, preventing from access of people to the data by changing the entering password or encryption such as crimes that are appointed in this category (Fajri, AlirezaCyber crime article www.pajoohe.com)[8].

Crimes related to content: this category involves crimes in which they are considered as the tool by criminal individual for committing crime, for example publication of illegal contents (Deziani, Mohammad Hassan, news related to cyber crimes, p.21)[9].

Some Criminal Responses to Cyber Crimes in Iran

Every crime has a series of main punishments that in the text of related law were referred to and a series of completing punishments and subsequent punishments that were specified in the law and in the case of the entire crimes depending on the idea of the judge the decree can be applied. To appointed sets that were discussed are called secondary punishments. Computer crimes are not exceptional and in these crimes when qualified the judge performs completion and depending punishments (JavidNia, Javad, crimes for electronic commerce, p. 247)[10]. In this relation, computer fraud about secondary punishments depends on generalities, therefore, in the case of main punishments only a level of punishment specified as follow:

1. Imprisonment from one to three years
2. Cash punishment equal to received finance

Also, decree for asset refusal is anticipated (Article 67 for electronic trade law)[11].

Punishment for fraud is specified as "the least appointed punishment in the article". In the case of appointed cash crime in this article the ambiguity is that if individual achieved no finance, but in article 67 of commercial law the punishment of starting fraud is appointed as "the least appointed punishment in the article". But it is not anticipated in the law of electronic commerce; therefore, it is not possible to refer to the article 67 of the e-business law to use it for starting electronic fraud. Article67 of electronic commerce law is in line with article 741 of Islamic punishment law (Aalipor, Hassan, ibid, p. 284)[12].

In the case of deficient right of author, the appointed punishment in article 74 of electronic commercial law is three to one year imprisonment and 50 million rial cash crime. In line with paragraph 2 of article3 of the law for some incomes of government and its consumption in specified cases approved in 1994, and verdict of unity the general procedure of general high court in this case is specification of punishments of imprisonment less than 91 days that is against law; but in specifying the punishment in article 74 this issue is not considered. In this regard problems of referring criminal laws to other crimes are totally clear. For example in analyzing article "the law of supporting authors, trades and artists" in a specific case that publication, distribution or offering the work to the name of author without the owner's allowance would be punished by six to three years punishment. But against international procedure that for deviating from the rights of author for electronic commerce according to drastic increasing of damages than traditional state more punishment will be considered and in article 74 this punishment decreased.

We should pay attention that violating the right of invention and attachments besides violating the right of mental ownership are indicated in article 62. But in electronic trade law it lacks specific application and they should refer to law "registration of innovations, industrial designs and trademarks". In this law against the law of the registering the signs and innovations in article 61 for violating the right inserted in the law, in addition to remedy damages by cash punishment from 10 million rial to 50 million rial or punishing imprisonment from 91 days to 6 months. In the case of representing trade secrets some punishments in articles 75 and 76 of electronic trade law are anticipated. By virtue of article 75 for violation from trade secrets 6 months to 30 months imprisonment or 50 million rial cash punishment. In

article 76 for violating trade signs the punishment is from 1 to 3 years imprisonment and from 20 to 100 million rials cash punishment. The main condition of occurring the instead crime is "in the bed of electronic exchange." It is possible that in line with crime we see violation from illegal access to crime, illegal listening computerized spy and in revealing some instances of trade secrets, violating the right of mental ownership to be the subject of article 74 of the law of electronic trade. Because some representations of trade business are supported by the law of "supporting the right of intellectual ownership."

For example, whenever a person having illegal access to a computer of one company that produces software, copy one of the software of that company and sell it under his name, then he committed three crimes, namely, illegal access, violating trade secrets, and violating the right of author that based on principle of virtual repetition will be enacted (Shahshahani, Siavash, legal issues of domain names, compillation of articles in conference of analyzing aspects of the right of IT, Tehra. Salsabil publication, first publication, 2005, p. 277)[13].

In the case of publishing falsehood in traditional criminal law for legal principle of this crime, article698 of the penal code. Publishing the falsehood in the law by letter compliant, deliveries, reports or distributing every type of publishing papers with or without signature as direct quotation from real or legal person or formal authorities to the extent that it is other than mundane or spiritual damage or not, in addition to preserving modesty that might be punished from 2 months to 2 years of imprisonment or lashes to 74 lashes (Mir Mohammad sadeghi, Hossain, crimes against security and general welfare, p. 234)[14]. Such cases if they exist in the cyber environment they are considered as publication of computer falsehood. In the case of crime of computer falsehood; article 18 of the law for computer crimes is appointed: "one who intend to disturb the public or formal authorities by computer system or telecommunication or try to make is accessible to others against reality, directly or indirectly to real or legal person might be related.

Whether based on the stated method by material or spiritual damage or no damage to other. In addition to recalling for modesty to imprisonment from 91 days to 2 years or cash punishment from 5 to 40 million rial or both punishments."

Punishment of "computer fraud" in the law of electronic trade other than position of fraudulent or damaged interest damage of "imprisonment from one to three years and paying cash for punishment as much as 50 million rial" is considered and in notice of the article for committing crime "the least punishment" documented in article 68 means three years imprisonment and 50 million rials cash punishment is appointed. According to the importance of this crime and according to the diversity of legal materials for crime traditional fraud in the Islamic penal code that considered different punishments for different types of fraud it is required to appoint punishment for different frauds like ensured electronic signature, faking the signature of Ministers, government companies and the same, not the realm of electronic trade that fraud imposes considerable damages using traditional statues, so the individual faces the slight punishments. In the article 6 of computer crimes, imprisonment from one to 5 years or cash punishment from 20 million to 100 million rial or both punish might be accused. Though article 68 is anticipated in the realm of electronic trade, but general title of crime and interpretation of "the bed for electronic exchanges" that is over electronic trade covers the entire electronic behaviors and result in misusing the law for computer fraud. This issue was continued to anticipating the law of computer crimes.

In the case of crimes against computer in line with article687, article 8 of the law for computer crimes was anticipated that here instead of materials data were issues to crime. Based on this article "one who illegally delete the data of others from computer systems would be punished to imprisonment from 6 months to 2 years or cash punishment from 10 to 40 million rials or both punishments." Also in the tenth article the law of computer crimes is considered clearly as crime. This article stated that "one who illegally by occurring some actions such as covering data, changing the password, or encrypting the data causes lack of access to legal individuals to the data or computer systems that they will be punished to imprisonment from 91 days to one year or cash punishment from five to 20 million rials or both punishments."

Cyber Crimes in International Documents

Activities of Cooperation Organization and Economical Development

The first attempt of international society in the case of discussing is one of the necessities of criminal law in facing computer crimes by OECD. Until activity of this organization there was no precise and comprehensive division. In September 1985 the specified committee of organization, advised that member countries that committed computer crimes should be followed by criminal regulations and the following committee for actions should be suggested:

A. Entering, changing, line or stopping computer data or computer programs that they will be committed intentionally for illegal transference of money or other things.

B. Entering, changing, line or stopping computer data or computer programs that are achieved for committing crimes intentionally or unintentionally.

C. Entering, changing, line or stopping computer data or computer programs or computer programs with other involvements in the computer systems that is intentionally or with the purpose of preventing from performance of computer or telecommunication system.

D. Having access to inclusive right of the owner of computer programs that are supported with trade productivity of programs and offering them to the market.

E. Access or cutting computerized listening or telecommunication system that is intentionally and without personal allowance, whether by offense tactics or other damaging or honesty purposes (Siber, Ulrich, the international handbook on computer crime, john Wiley and sons , p. 92[15]).

European Consultation Activities

European council according to the issues of civil freedom, personal law and legal support of interests and legal properties will not be supplied by OECD and it is possible to study these issues with respect to technical and legal views to offer guides for helping legislators to specify behaviors that can be forbidden according to their criminal rights. One of the sections European Council is European committee of criminal issues. This committee is an expert committee to study these issues. This committee started its work in 1985 and terminated it in 1989. The basis of working for committee was an answer that was offered to member governments and a report that was offered by OECD. Beside the offered reports, experts and consulters of guidelines for national legislation. Different types of computer crimes were defined and some descriptions about them were offered (Pakzad, Batol, ibid, p.60[16]).

Activities of UN

This organization prepared a committee entitled as preventing crime and treating criminals several years a year. In the seventh congress of UN that was hold in 1985 including stated issues in the report of the UN Secretary General about the issue of computer crimes. Then in the conference of European area it was suggested that international campaign with computer crimes by eighth congress, agent of the Canadian congress, offered the text of the charter about computer crime. This text was approved in thirteen conference and some suggestions were offered to the member government. Also it should be stated that in the approved text definitions and divisions from OECD and European Council were emphasized (Newsletter of Informatics, No. 61, p.213[17]).

Activities of International Association of Criminal Law

The international institution of criminal law is a non-governmental organization that is active for more than one century. This institution with preparing an international congress that will be hold once a year in one of the member countries in 1990 institution posed four subjects that we can refer to computer crimes or other crimes against information technology (Shirzad, Kamran, Computer crimes in the view of Iran's criminal law and international law, p. 48[18]). International institution of criminal law in 1992 and 1994 established congresses that approved European Council and accepted its division. For many progresses and for increasing the sensitivity in some cases some fields need more attention. Therefore, crimes can be divided into independent crimes in the list of European Council. Respecting this institution issues that independently should be stated are: violation related to the passwords, publication of virus or similar programs, access to mysteries against law, applying, transferring, and illegal changing of personal data (Newsletter of informatics, No 61, p. 220[19]).

Convention of cyber environment crimes high council of legislation development of the committee of campaigning against computer crimes member of European Council and other conventions having considered this issue that their purpose is having access to the objectives of European council for greater unions among members with respecting development of cooperation between members of convention believing in necessary need for them as a priority for the same general criminal policy in supporting society against crimes in the cyber environment and approves appropriate laws for cooperation and by having information about main changes that are formed by consequences of digitalization, coordination and globalizing computer networks and being worried about a danger that may use computer networks and electronic information in doing crimes and reasons related to such crimes that were saved by such networks or those who were transferred and cooperation between governments and private industries in the case of campaigning against crimes of cyber environment and need for protecting legal interest in usage and developing information technology and the belief that influential campaign against cyber crimes needs increasing and fastening a desirable performance in international cooperation with respect to criminal actions, and criminology is necessary so that present convention preventing applications that are the reason for secret, totality, and accessibility of computer systems, networks and computer data, might be misused (www.bashgah.net.[20]).

Global Declaration of Human Right and International Contract

By human right regulations we mean principles and norms that are reflected in Human Right Declaration (1948) and international contract of political and civil law (1966). Three principles of these documents considerably were affected by cyber environment that were dealt with. The effect of cyber space on freedom of expression: in this case article 19 of declaration states that: one who has the right of freedom of expression this right requires that they should have no fear from expressing their ideas and in receiving and establishing information and thoughts by entire tools without border considerations they should be freed.

This article is very clear and comprehensive and it is not required to interprets and update it and in every possible time and conditions everything is appropriate.

The Effect of Cyber Space on Free Flow of Information

One of the principles that emphasized in international documents of human right are in line with freedom of expression are called free flow of information. Doubtless freedom of expression will be achieved a time in its real meaning to establish information without any limitation in the society. 3. The effect of cyber space on private space: in this case article 12 of Human right article states that private life, family affaires, house or people's communications should not be interfered directly or their modesty and fame might be offended. These people have the right against such invasions from support of law. Article 17 of contract is similar (Jalali Frahani, AH, preventing cyber crimes beside human right regulations, Journal of law and jurisprudence[21]).

Deficiencies and Legal Gaps

Laws of Islamic Republic of Iran's Computerized crimes and law of Electronic trade and other related laws to computer crimes beside having many benefits that have many deficient. In this case anticipating the title "crimes against general modesty and ethics" instead of crimes related to the content and the title is ambitious, but measuring the cyber space with external space and modesty and general ethics in cyber space has no general and global root and cannot be accepted. In other words violating the modesty in general view would be happened in the public, while cyber space is a personal space so that in the general space we can see that in this space the general modesty and ethics is incorrect and do not need legal bedding and specification of lexicon (Aalipor, H, ibid, p. 387[22]). Also under-predicting forgiving of the compliant in some computer crimes that their general feature is dominant is one of the weak points of this law. Forgiving should be predicted in the law or without achieving at this principle it is supposed that crime is not forgivable. In the law of computer crimes, most of the crimes like destruction, illegal access, publishing private pictures and family issues has a private feature and some others like fraud, spy and listening can be along with emphasizing on private aspect. Therefore, forgiving of the plaintiff is most of the computer crimes might be effective.

Referring to the laws of computer crimes in the situations of crime and specifying punishment is just for those crimes that were predicted in this law, otherwise if there is a crime like offense in the internet based on the related law it would be investigated by law, because computer or internet are crime when they are equal to crime, therefore, article 22 anticipated that: "in cases that computer site or telecommunication site are used as the means of committing crime in this law there are no specified action for punishment, and based on criminal law they would be behaved." In the case of formal appointments the same issue is dominant; because the law only deals with separating aspects and other formal propositions should be based on principle aspects. Based on notice of article 52 in the cases that are not anticipated in computer crimes of specific regulations with respect to judgment regulations; according to the rules of judgments punishment will be enacted, that it is itself a deficiency for the law (Aalipor, H, ibid, p. 391[23]).

CONCLUSION

As the area of affectivity of crimes that happen in cyber space are wider than traditional crimes and consequently damage would be directed to them, therefore, as mentioned communities resist against occurrence of crime in the physical world, and they would offer strategies appropriate for preventing resistance against occurrence of crime in the virtual environment that has different features than real environment and it is a necessary issue. This article tried to analyze cyber crimes in Iran's law and international documents. In criminal view, qualitative and quantitative distinctions of cyber crimes than traditional crimes faced affectivity of common criminal system with serious challenges, so that scientists in the realm of law and policy makers in the related fields should ponder and decide about some important issues. The most fundamental point about criminal law and criminal policy is quantitative and qualitative differences with crimes of real world. Speed, plurality, simplicity of commitment, cheapness, internationality, unfamiliarity of commitment, automation of crimes is of these distinctions. Most of the countries for newness of achievements of this technology have to pass classic principles and by accepting at least a part of suggested lists of international organizations tried not to be away from information and functions and by approving domestic laws and attaching to the convention of cyber crimes are involved in the global process of this achievement. Therefore, we should pay attention that criminology merely and specification of criminal application is not sufficient and criminal tactics are influential against crime if it is possible to follow crime.

Therefore, as in the cyber space the basis is unfamiliarity, in most of the cases detection of committed crimes and punishment in the national and international level faces challenges that in this way education and increasing the level of education about cyber space should be considered. In addition, increasing dependency of economical substructures for developing cyber crimes and developed damages that appointed to such substructures. On the other hand, needs a criminal policy in different dimensions of controlling, managing and prevention. Based on the importance and development of computerized crimes especially crimes of new generation would have an international nature respecting the method of commitment would have a totally new nature with respect the criminal dimension that challenges national and international activities that emphasize on the following issues: in the new legal fields comparative studies and international cooperation should be developed more than before. Especially in the case of trade mysteries that are supported by criminal law, support of criminal law from computer violations to private and personal laws and specific issues of computer crimes, network and international crimes should be considered seriously.

- Cooperation with international society in the case of related law, formal and international issues, cooperation with scientific circles and exchanging thoughts and experiences
- Attention to legal article causes lack of criminals escape and their attorneys from justice and considering the entire conditions of a type of criminal policy.
- Laws should be considered deeply to study damages of computer crimes than traditional crimes in the case of increasing the type of punishing criminals.
- Also, it is better to specify the people's criminology, whenever violating to the space of others that should be punished legally.

REFERENCES

Alipour H (2011). *Criminal Law*, first edition (Information Technology Publications pleasure).
Bastani B (2004). *Computer Crime and Internet Crime Novel Effect* (printing, publication, B).
Cushion Morris (No Date). *Principles of Criminology*, translation Ayatollah Sadiq (Tehran, Justice).
Dezyani MH (1997). *Cyber-Crime*, **I** (the Secretariat of the High Council of Informatics).
Fjry AR (No Date). Cyber crime. Available: www.pajoohe.com
JalaliFarahani A (2004). *Prevention of Cyber Crime in the Light of the Situation of Human Rights* (publication rights law).
JavidNia J (2009). *E-Crime*, second edition (published by Khorsandi).
Lazrzh Christian (2003). *Introduction to Criminal Policy*, translated by Ali Hussain Najafi Abrandi Abadi (Tehran, publication of the Spring).
Marty MiriDlmas (2002). *Major Systems of Criminal Policy*, translated by Ali Hussain Najafi Abrandi Abadi (Tehran, emission rate, autumn).
Mir Mohammad Sadeghi H (2008). *Crimes against the Public Welfare, Emission Rate*, eleventh edition.
Najafi Abrandi Abadi, Ali Hussain and Beigi HH (2011). Encyclopedia of Criminology.
Newsletter of Informatics, No. 61, p.213
Pakzad B (1996). Computer Crime, Criminal Law and Criminology. Master's thesis, martyr Beheshti University, Tehran.
Shahshahani S (2005). Legaldomains. *Proceedings of the Conference Paper Review the Legal Aspects of Information Technology*, first edition (salsabil Publication) Tehran.
Shirzad K (2009). *Computer Crime from the Perspective of Criminal Law and International Law* (Iranian, printing, publishing a comprehensive SEO Company).
www.bashgah.net