Iran Criminal Policy Due to Electronic Crimes

Fatemeh Nouri

Abstract— One of the most dangerous crimes that compromise socio-economical and political securities of the society is electronic crimes that have been manifested in the world era with its modern forms simultaneously with development in science and technology so the only condition for fighting against modern crimes and their prevention is to identify, analyze and recognize completely how they are committed. At the moment, in one hand there is no sufficient equipment in order to resist against crimes, on the other hand modern criminal policy does not have enough cognition and knowledge in order to fight against this new offenders. This study is aimed to explain concept of computer crime, identification of specifications and its different kinds and investigation of present legal solutions and indication of possible defects regarding high speed computerization of commercial-industrial and servicing activities in Iran.

Index Terms— Cyber crimes, informatics, communication technology, communicational networks, computer systems, criminal policy.

1 INTRODUCTION

BY entering to a meta- industrial society (informational), twenty's century has been faced with modern challenges in many life areas. This change has been occurred not only in the science but also in economy, policy and law so computer and communication technology have been followed by many professional discussions. Today, Information technology includes most of daily life especially in industrial countries; computer has been changed into an inclusive and essential tool in human lives and its usage in all fields is being increasing including scientific researches, medical affairs, finance, industry, and policy. Although, this technology has brought about countless advantages for governments and citizens, it causes many social, economical and judicial problems. Increase in computer abuses and imposed losses have made different people such as criminologists, lawyers and computer experts to study all aspects of this event. Of the most important and current computer crimes are as follows: fraud in credit cards, fraud in telecommunication lines, using computer for personal affairs by the personnel, non- authorized access to computer files due to curiosity, illegal copying from protected software and so on. This kind of crimes is being committed in a professional way that a considerable percentage of them cannot be identified. Today, judicial systems in the world in one hand face with growth of computer crimes and heavy losses remained from them and on the other hand, due to problems of legal regime present in countries, there is no power to prevent them effectively. It is while that everyone can commit this kind of crime against every citizen and maybe there is no crime such as this one regarding criminal motivation, kind of crime and its effective intensity. So it seems that the first step is to recognize the concept and topic. The main question is whether there is any difference between traditional crimes and computer ones regarding degree, volume, quantity and device or there is a fundamental and natural difference. On the other hand, can it be said that only the tool and space have been changed? If the former is true, it will be possible to fight against computer crimes by principles and basics of current criminal policy. Theft, for example is theft but only the device of committing crime has been changed or in swindling, only the fraudulent device for carrying property has been changed and the nature of theft and fraud and how to commit them may be different in computer world. But if the latter is true, the current criminal system with present principles and strategies is not able to realize its objectives in direction of fighting with modern crimes. In this study, it is tried to analyze and study criminal policy regarding these crimes. In order to reach this goal, patterns and models of crime act will be discussed in two different spaces.

A: how to act a crime in a traditional model

One of the most important features of crimes in a real world is that in general a kind of positional proximity is necessary between criminal and victim. Theft, pocket picking, adultery, murdering and many other crimes have this feature meaning the criminal has to be close to the victim in order to act the crime. The second feature is that a criminal has a conflict with the victim while acting the crime and after crime completion; the offender can commit other crimes. His or her planning and goals focus on the crimes that he or she wants to act. Forger plans for forging a document and makes it then he acts other crimes. The third is that crime act in a real world is a function of physical limitations meaning that each crime even the simplest one such as pocket picking and street crimes needs initial readiness, planning and implementation. The more complicated the crimes, the more limitations. In simple words, traditional crimes have many limitations even after acting them regarding sale concealment and property transportation and so on. The fourth feature is that crimes are occurred in certain places of a city so

• *Department of Law ,Payame Noor University ,Po Box 19395-3697.ir.ofiran*

legal entities are able to centralize its forces and sources in possible places of crime act and show proper response and reaction against them. These features show that cyber crimes are as a new kind of crimes and have their own characteristics that distinguish them from other crimes. Later we will discuss them.

B: how to act crime in cyber crimes

In cyber crimes there is no necessary physical adjacent between criminal and victim. It is an unlimited crime. The criminal and victim may live in different cities even different continents. The only thing that a criminal needs is a computer system that is connected to an internet. By this simple equipment, he can attack victim's computer and commit a fraud or get personal information that enable him to commit criminal actions in a wide range by forging others' identity. In cyber world, the crime will be committed automatically by technology. This allows criminal to commit thousands of crimes with a very high speed without any legal threats and attention of the victim. So it is not possible to escape or take necessary actions that are existent in traditional crimes. On the other hand, criminal results and software and tools will be destroyed immediately after committing the crime so it is impossible to resist against them and state criminal law and procedure law face sever challenges in order to fight with these crimes.

2 PROBLEMS OF FIGHTING AGAINST CYBER CRIMES

1- In traditional crimes, pyramid model is used meaning report of criminal event, taking command for enquiry and prosecution, inspection and issuing sentence and executing punishments while in cyber space but it is impossible due to networked crime, speed of its committing and anonymous criminals

2- Lack of a certain borderline while acting the crime

3- Removal of evidences of crime act

4- One of problems in prosecuting and arresting criminals is that they are anonymous and unknown in cyber space. Face off and identity changes by makeup, plastic surgery, document forging existed in traditional crimes are not comparable.

5- increased crimes in cyber space is another problem because most of famous national and international companies do not want to show their unsafe business activities by disclosing acted crimes in order to not destroy their credits.

6- Cheap cyber crime: the most important device is a computer and telephone line in order to connect to the internet

7- Lack of international coordinated rules regarding definition of unit of cyber crime and judicial cooperation is one of the basic problems that needs long term international steps

By investigating these problems, it should be said that criminal policy has to have two main strategies to face cyber crimes.

3 STRATEGIES OF CRIMINAL POLICY

3.1 Reactive strategy

Reactive strategy means action taken after crime act which is inevitable and undeniable one in all crimes. It has no certain function in cyber world due to its unknown range, rate of crime act and problems existed on the way of discover, proof and judgment.

3.2 Strategy of prevention, control and management

Traditional crimes are a network organized for making human force and source but internet is a new social network that needs a modern criminal policy with a new preventive and controlling strategy meaning it requires active participation of all effective sections such as government, private sector and all people who are affected by cyber space. The most important preventive, controlling and manageable strategies for cyber crimes are:

1- Civil responsibility

All producers, importers, distributors and even users can be responsible for incorrect usage and production due to ignorance resulting in damage and losses to people of the society. Responsibility resulted from vicarious liability, citizenship responsibility and intensity of cause to preparation are not unknown entities in our legal system because negligence in making software tools and computer systems and not considering safety points can cause damages and losses to people, ethics and social credits (Katouzian, 374-1377:390) for example not considering safety points by a user and stealing of his device password can be an open window by which others' property can be stolen simply without identification of the criminal. So the user who has not been careful enough in protecting his device can be liable.

2- Criminal liability

The next step is to use vicarious liability in criminal dimension. The person who is able to control aggressive actions of others especially a person who benefits from those actions should be liable legally and criminally. It includes producers, makers, and designers of computer systems, providers of internet service and internet connection points.

4 Conclusion

We concluded in this study that today wide possibilities of computers not only have attracted good people but also criminals in a way that security forces face several crimes committed in internet network. There are many problems regarding prevention and persecution of these crimes and the current tools in criminal law cannot respond these problems so professional debates have been made in parallel with development of different kinds of computer crimes and international organizations have taken concentric actions in all countries in order to solve the problems but it is not enough so the most important thing for defending information networks against attacks

is to consider security points by increasing security of networks, installing protective systems and precise systems for discovering hackers and development of security software tools. In addition, all people working with computer should be familiar with issues related to computer especially judicial officers should be trained to cope with inspection, collection and protection of computer evidences. In general, it can be said that criminal policy effective for fighting against computer crimes and preventing them should be based on following principles and rules:

1- Supplying trained forces and establishing legal centers equipped with computer under control of the legislative power in order to discover crimes, collect evidences and enforce law of identification and prosecution of criminals.

2- Crimes of damaging behaviors in cyber environment

3- Crimes of initial actions

4- Informing companies and departments regarding ability of risk taking of computer systems and encourage them to use security measures

5- Promoting standardized security measures

6- Decreasing criminal situations and opportunities of using technical tools in committing an offence

7- Encouraging the victims to acclaim the criminal occurrence

8- Formulating proper rules and doing necessary amendment in current regulation of the country

9- resorting to international cooperation for discovering computer crimes and prosecuting criminals of these kinds of crimes. In order to resist against cyber crimes, the second liability is a better solution because sometimes those actions that do not cause damage naturally but can result in damage, should be recognized as crimes. For example, non authorized access to the system and information available in the computer should be placed in list of crimes because it is the first step in committing cyber offences against others and non- authorized access to information available in computer systems. This action has been recognized as crime in cyber offences convention in 2000 and English law of abusing computers in 1990.

REFERENCES

[1] Ashoori, Mohammad, the book, introduction to internet and computer crimes, a new manifestation of criminal, Behnam press, second edition, 2007, p 13.

[2] Katoozian, Naser, civil law in current legal order, Dadgostar press, 1998, Tehran

[3] Ashworth Andrew, principles of criminal law clarendon press. Oxford 2000

[4] Rosenberg Jonathan, cyber law THE LAWOF THE INTERNET, spriger USA 1997

[5] Smith and Hogan, criminal law, ninth edition batter worth London, Edinburgh, Dublin 1999

[6] Susan w. Brenner opcit.