IJBPAS, September, 2015, 4(9), Special Issue: 379-390

ISSN: 2277–4998

International Journal of Biology, Pharmacy and Allied Sciences (IJBPAS)

'A Bridge Between Laboratory and Reader'

www.ijbpas.com

DIFFERENTIATION OF PENAL POLICIES FOR CYBERCRIMES (WITH A VIEW TO IRAN'S PENAL LAW)

[1]MOHAMMAD KHALIL SALEHI, [1]MOHAMMAD ALI HAJI DEH ABADI, [1]DAVOOD KARAMI GOLBAGHI

[1]Qom University, Iran

mohamad.salehy@gmail.com; dr_hajidehabadi@yahoo.com; karami.law@gmail.com

ABSTRACT

Cyberspace and information technology have influenced deeply all social, economic and cultural aspects of life as well as penal laws. The difference of cybercrime with conventional crime is in such manner that usual approach and known basics and principles are not able to confront against challenges of such crimes. Internationality, easiness in committing the crime, and anonymity of offenders is among certain feature of such crimes. Mentioned features from one hand and dependency of modern lifestyle to cyber technology from other hand necessitate to specify a different penal approach. Effectiveness and efficiency of laws that are approved for confronting cybercrimes entailed a different view to issues such as crime definition, crime components, and penal responsibility and so on. The subject of current research is reasons and requirements of presenting a differential approach for penal laws against cybercrimes. In this regard one attempts to analyze some case of differential approach in Iran Islamic penalty law.

Key words: differential approach, conventional crimes. Cybercrimes

INTRODUCTION

Information technology superstructure has created a new world that is different from real world. There is no Private owner and government. Internet does not comply global regulations. There is no general or public legislator. Though some attempts are taken place in order to developing legislation in number of multilateral authorities. However the cyberspace is described often as a lawless, unlimited,

chaotic, uncontrolled and accessible environment. Information technology and communications not only influenced industry, economy, commerce and other areas but also leads in these changes in the area of law too. Following these essential changes naturally lawyers similar to other expert should present regulations and legal principles and laws for preventing or settling conflicts arising from such changes to be consistent with technology and preventing to lose the pace. This new space is so that the conventional penal rights is sustained fundamental changes so that definition of crimes in cyberspaces has no such accordance with classical definition and it is quite deferent in many aspects.

Another important point about cybercrimes is their exclusive features comparing with conventional crimes. Speed, frequency, ease of commit, cheapness, infinity, anonymity, automaticity and so on in digital crimes leads in rise of different type of crimes. Mentioned features from one side make it easy to organize and engage in an attack remotely from offender and from other side ever-increasing dependency to economic, industrial, service, security and political products to cyberspace encounter human society to stern threat. In such manner that official reports of United Nations did not reckon any area of human life as safe again cyberspace threats. Cyber organized attacks can encompass all socials infrastructures and even target national security. Such crime with such expansion and exclusive features requires special strategy in various aspects. This strategy can include extensive measures in diverse aspects of penal control, management, preventive and reaction. Present research is engaged in one of dimensions of mentioned measures namely, selecting differential penal approach in penal laws.

Though prevention from cybercrimes is more effective than substantial suppress and confrontation and there is different tools and mechanism for controlling such behaviors. But penal confrontation is just one of usable methods. Nevertheless for different consideration and based on available reasons and evidences it is essential to support punishment for the violated values. The penal system should manage to increase hazard of detecting and prosecution of crime and condemnation as well as appropriate and inhibiting penal reaction so that convince cyber offenders who are often careful and thoughtful in such manner that prefer to refrain from committing crime acts. This function requires to adopt an integrated an directed penal policy. Because cybercrime are committed by complicated and new methods and the way of committing such crimes has sustained a fundamental change.

Specifying penal reactions in penal laws follows generally common principles and basics. In determining and definition of delinquency and its components and penal responsibility basics and its governing regulation one acts in such manner that it would have a more or less similar application toward various types of delinquency. For example all crimes have three component and slight and intense qualities exist among all crime in more or less similar manner. The same common feature can be observed in the form dimension too. In this regard the regulation governing on delinquency detection, prosecution, trial and exerting penalty against delinquency have comment bases. Policymakers in penal area attempt to adopt equal rules against all kinds of delinquency for realizing justice and protecting individual rights and freedoms. For example rules about accused rights, the reasons for approving the delinquency, accused arrest and summon, legal procedure and so on have similar norms.

But sometimes society interest, certain feature of offender or victims or extensive effects that some type of delinquency brings about in the society lead in a situation where the legislator enact some norms different from usual norms with regard to some exceptional cases or for the same reason it clarifies some different regulation different from usual legal procedure. Some patterns of such differential penal approaches can be observed in cybercrimes. Therefore in current paper at first one seek to find special features of cybercrime so that by this attitude we can reach to differential penal policies manifestation in territory of these crimes.

Special features of cybercrimes

The fundamental question about cyberspace is whether these cybercrimes differentiation from conventional crimes is matter of situation or intensity? In other word the differences between them is out of quantity or quality? Does merely the space of crime commit, tools, speed and volume of crimes have sustained change or essence of these crimes sustained alteration as well? Can one consider these changes as combination of qualitative and quantitative changes? In first state that the premise is that tools and environment of crime sustained changes with traveling from conventional model to digital space, thus one can settle these challenges by insignificant changes in penal policies. But if these differences are product of fundamental and essential changes or combination form first and second type, for addressing new requirements of virtual world it is indispensable to build a differential approach.

It seem that the changes emanating from cyberspace appearance is different from changes arising from other complicated and modern technology. Though transportation industry, communication, weapons and other industries and technologies have stimulated special delinquencies, but since these changes are typically at quantitative aspect the penal justice system directs itself with higher speed with requirements arising from modern structures. It means using present-day principles and basics of penal laws attempts to confront the crimes in form and content aspects is fairly successful in this regard. But features of crimes in cyberspace suggest that penal laws should enter a new stage in form and content aspects. In such manner that just the prerequisite of defying such crimes is presenting a new analysis about the manner of committing cybercrimes and building an appropriate penal approach.

In current era the matter is not merely about that there is not sufficient equipment for confronting ever-increasing cybercrimes or that velocity and acceleration in computer and information science and usage of network does not give time to us for developing defensive system against attack or preventing them. But even accelerating in current judiciary system preparations for confronting such new wave of delinquency is not sufficient completely. Claim of current paper is that realizing confrontation objectives to cybercrimes ensues clarification of certain kind of penal approach that is not equal to conventional penal approach. Identifying and analyzing cybercrimes features and characteristic and consequently special committing model clarifies the necessity of building such approach.

Volume and scale of cybercrime

Real world crimes characterized by the fact that the crime model follows the norm of "one-to-one". In other word an offender usually is involved with one victim. In essential crimes such as murder, rape, the fire and so on the offender usually target one victim and all its attention is focuses on accomplishing that crime. When the crime has been accomplished then the offender move to other victims or crimes. The rule of "one-to-one" in real world crimes is arising from imposed physical limitation on human activities. A thief cannot steal at the same time more than one wallet. Therefore real-world crimes are serial crimes. In addition, the offender and victim generally live in a same town or district and the offender identify its victim already and then commit the crime to it, therefore this is an appropriate opportunity to recognize or detect the offender by victim. If the offender and victim have not social relations or in other term they are stranger

to each other the unfamiliarity of offender increases probability of identifying the offender and local citizens greatly help because they pay great attention to a new arrival in the locality. Therefore the researcher for a conventional crimes essentially is concentrated to a certain geographical locality where the crime has been taken place [1]. These limitation allow to the penal justice institution to predict necessary planning for confronting the crime and offender. But in cybercrime the rule of "on-to-many" is governing. Therefore victimizing thousand and even millions of people within a single measure is a true and credible assumption in cyber space [2]. This leads in that amount and number of delinquency is not comparable with digital and real world. For example in 2002 in Unites states more than 90% of industrial enterprises sustained cyber-attacks and hundreds of million dollars sustained damage [3].

Anonymity in cyberspace

Anonymity is one of governing rules on virtual space [4], and it is emanating from intangibility of this space. In this environment one hides its identity behind its computer, and finds a safe and secure environment to perform whatever it wants. Because there isn't blaming look of police and people to dissuade them by fear from arrest or shame. Concealed environment of cyberspace allows to the such persons to manifest hidden part of some humans that does not find room in the society to manifest them and this remark of intellectuals such as Hobbes that consider human nature as evil would be fostered in such spaces, because it is sense of concealment of crime measures that shows the internet as a free world so that one can indulge itself rebelliously and free from social and moral controls for committing wrongdoings. An example for this is presented pornographic image of children in cyberspace so that from one side it provides profitability for who present such images and form other side it provides a free and vast world for someone who want to satisfy their sexual drives so that in any time they enter this fantasy world and subside their intrinsic drives.

However the meaning by anonymity of this space is not that one cannot observe it but from one side identifying users connected to the network is essential complicates and expensive, Form other side intrusion to other users' information, online concealment and other types of disbursement make it difficult and sometimes impossible to identify offenders. These crimes are mostly happened before informing legal authorities and even the victim itself and traces of crime and used software is eliminated immediately.

Therefore this space is always coupled with vast range of countless, scattered and anonymous offenders. There is Capability of information spontaneous exchange in tremendous volume in this space. This feature is not found in other mass communication tools. Also multimedia feature separate this from other phenomenon as a quite exclusive one [5].

Users can choose information in cyberspace. The search and exploration ability make them able to receive any information they desire and contrary to other media that information is imposed to target and there is no occasion for choosing information, the flow of information is not one-sided, unidimensional and imposing.

Manifests of differential penal policies in Iran computer crimes law

The purpose of differential penal approach in this area is taking a different but strict approach against cybercrimes versus customary crimes. The purpose is not that this approach should be quite different and all solutions would be innovative and special for this kind of crimes. The claim of this paper is that the effective penal reaction model in this area is to adopting more extensively the set of legal technics that either they have no application in conventional crimes area or are adopted exceptionally. In fact some technics are innovative or some other are exceptional and scattered measures available in real-world and are used systematically and purposefully in cyberspace, lack of support from neglectful victim, usage of concepts such as vicarious liability and absolute liability, developing legal entity penal responsibly, criminalization of preliminary acts, identifying the beginning of the crime as a complete crime, developing absolute crime, identifying act dismissal as corporeal element of crime, developing complicity concept, reducing crime component and so on can be considered as components of differential penal approach of essential law in virtual space area. This writing is a topic of how to use these concept and adopt them in penal laws such as regulation of Iran computer crimes approved in 2009.

Homogenization of criminal behavior

In conventional crimes due to different settings of crime action and different criminal shapes of scenario the corporeal element of each crime naturally is different from other one. The fraudulent person with putting on a justified air and appearance and by fraudulent plans may cause someone dliver its property to it for example by establishing a fictitious firm. In first generation cybercrime though the crime corporeal element didoes sustain such change and have great similarity to classic crimes. But in third generation these

similarities waned and it turned into relatively ownership of crime devices.

In cyber fraudulency the offender does not deal with its victim directly even maybe it does not know the victim, the fraud take the possession of victim such as cash or bank storages through false computer program. He does not deceive any person directly. Then in the definition one should take this into account. Secondly during conventional fraudulent crime the operations committed by offender such as establishing a fictitious firm, giving hope for nonrealistic issues, scaring from unrealistic issues and so on but in cyber fraudulence the offender does not deal with owner of property or aforementioned physical issues. It thoroughly deals with information and computer systems and by false program or data changing or any other similar cheat take possession of some properties in bank computer system or other economic, financial commercial institute and so on. The law context in classical mode is established thoroughly on physical behaviors and interaction of offender with victim. This aforementioned issues is in accordance with article context, but these matters cannot be included at all in data processing operation range. Thirdly, over time and progress of information and computer technology the diversity of cyber fraudulence operations is fostered. With a look to change path of fraudulence one can observe such revolution. The cyber fraudulence by traveling from offline system to online and internal to international domain enjoyed such great changes. This in definition of cybercrimes one should take into account the whole image and present a definition that accommodate all new advent cases.

The article 741 of Islamic penalty law describe fraudulency as: "anyone take possession of cash or property or profit or services or financial patens for itself or someone else in illegal manner through computer or telecommunication systems with committing actions such as inserting, change, elimination, producing or ceasing data or manipulating or disturbing a system". Therefore at first according to this article of law the corporeal component of fraudulence is redirected from manipulating the person or persons to the machine and is engaged in systems data processing without addressing operator of such machines. Secondly insertion, change, elimination and interfere in program or system performance should be taken place in order to misleading the system. With such definition at current time one can legally punish these offenders. This is the same case about forgery. the article 523 of Tazir law approved in 1996 states:" forgery and fraudulence is: making a script of document

or seal or signature of persons scratching or scraping or manipulating or connecting or eliminating or blacking or advancing or delaying a date and so on" that all of them emerge in paper and pen and material and corporeal devices and have obvious difference with forgery corporeal element in cyberspace that include electrical or optimal impulses. The mentioned crime corporeal component in article 734 of Islamic punishment law approved in 2013 in computer crime part is stated as:' anyone commit following acts illegally is considered as forger:

a) Change or engendering documentable and reliable data or fraudulently producing or inserting something to them
b) Changing data or existing signs in memory card or digital cards in computers or telecommunication items or chips or producing or inserting fraudulently data or signs to them".

in forging the desirable purpose of forger is that by credit of air of document make it as a desirable nature for obtaining profit and the delinquency is obviously focused on the forged document, while in fraudulence crime the focus is to deceive the victim or operator of data processing machine even though it is possible that in this procedure one commit some acts such as forgery. So in computer forgery misleading the system or computer program is not the target but "change", "insertion" "producing" and so on of crime corporeal element is taken place. Therefore the cybercrime is part of crimes emanating from modern technology, unnatural crime where sometimes the computer is tool and sometimes the goal and other times the matter of crime but it is considered typically a type of crime. Speaking of content sometimes it has descriptions and titles of classic crimes due to difference in corporeal components and it stands out from classical crime category and finds compound titles. For example computer fraudulence and sometimes computer crimes have new titles, suggesting how the information technology is (that are often new generation crimes in cyber space) and their feature is the type of corporeal component of crimes is quite special. Development of these crimes changes the governing rules on classic crimes and from other side requires new supports of penal laws. Support from information and thinking ownership is a new topic in law and is arising from pattern change of support from objectives and objects and tangible matters into intangible and virtual items. Therefore the cybercrime subject can be others property, public safety and wellbeing, individuals, public ethics, computer information and data. And

they are very more extensive than matters of classic crimes.

Cybercrime corporeal component are almost homogenous, it means its components usually include intrusion, change, eliminating, halting, manipulation and so on in information, data, program or computer systems and remote communication networks. The same feature in corporeal components leads in emerging difference in cybercrime to conventional crime. As it is mentioned before in cyber fraudulence insertion or change of financial data lead in funds transfer and in fact property of someone else is stolen without that the victim would be deceived directly or even encounter the offender.

Preliminary acts as crime

In conventional penal laws the continuum of delinquency occurrence starts from delinquency action imagination and tendency to do it and then providing tools, carrying out preliminary acts, beginning the crime and accomplishing it. In penal systems fundamentally the preliminary acts are not reckoned as the crime. In Iran penal system even beginning the crime is not essential the crime. In exceptional conditions due to importance of the crime and expansive effects of certain crime maybe the penal policy is based on that the beginning of crime is considered as the crime and or in more acute condition the preliminary acts is considered as beginning of the crime or complete crime.

In cybercrime due to its expansive effects, complexity and difficulty of crime detection, identifying the offender and approving the crime, the penal policymaker has taken a strict position and intended to stifle the crime at beginning. For the same reason it defined the preliminary act of crime not only as the beginning of crime but also as an independent crime. The article 732 of Islamic punishment law specifies as:" anyone intends to access confidential data to violate the matter of this article (confidential data in transferring or storage) is condemned to imprisonment from 6 months to 2 years or financial punishment from 40 million rials or both of punishments:.

Situation of Conduct crimes

Crimes are divided based on corporeal element into two groups of result crimes and conduct crimes. The crime is termed as conduct because the criminal feature is belongs merely to appearance of the act and in defining punishment occurrence of harmful result is not taken into account. For example view to first part of article 518 of Tazir law making coins similar to gold and silver coins is punishable and it isn't necessary that the coin maker consume the coins or benefit from them. Or when legislator consider the exam paper leak as

crime (single article of law of examination questions revealing approved in 1938) it paid attention to way and manner of accomplishing the act and never take into account the outcome and result of the act. But if the legislator takes into account the outcome of crime such as murder or theft, as long as it didn't put an finish to life of someone or didn't take the possession of someone's property the crime is not accomplished. Therefore realization of outcomes inseparable part of crime and without emerging the outcome, the crime is not realized. Such crimes are known as result crimes.

Among reasons of defining the crime in the form of conduct is selecting approach of intolerance against such crimes that have more sensitivity and have expansive consequences. In computer crimes law in line with taking deferential approach, a trend to defining crime as conduct is obvious. Samples of such approach can be observed in article 729 of mentioned law as illegal access to computer system data, illegal eavesdropping (article 730) safety measures violation (article 732) and computer forgery (article 734). Among mentioned cases the mere access or illegal eavesdropping or violation of security measures regardless to eventual results or benefiting or harm are considered as crime.

Reducing crime components

One of reasons of taking differential but strict approaches is reducing crime component. Because as the number of crime components increases, the crime proving is more difficult and therefore confronting the offenders would sustain more limitations. For example the conventional fraudulence is a result crime. Many elements such as fraudulent devices, deceiving someone else and taking its property is necessary for its accomplishment. In such crime from one side numerous corporeal elements should be proved and from other side knowledge, public ill-will and specific ill-will of offender associated with mentioned corporeal elements should be evidenced. Failure in prove or hesitation in realization of each one of corporeal or abstract components of mentioned crime is an obstacle for proving the crime and in other term it is a loophole for offender for escaping from punishment. Therefore despite of persistence of legislator for intensifying confronting delinquency fraudulence in law of intensifying bribe giver punishment, embezzlement and fraudulence approved in 1988, diversity of mentioned elements is a serious obstacle for confronting fraudulence.

The article 741 of Islamic punishment law is appointed to computer fraudulence comparison with conventional fraudulence

and suggests that the crime component in the first comparing with the latter is reduced significantly. For example in mentioned article, there is no trace from resorting to fraudulence devices and deception for realizing computer fraudulence. It is natural that in psychological aspect the crime component is reduced with the same proportions.

From other side the necessary outcome for realization of conventional fraudulence crime just has one case and that is taking someone else's' property, while outcome of cyber fraudulences includes significant extension. These results include property, benefit, services or financial patents for itself or someone else. From one side the cyber fraudulence crime component element and from other side the legislator avoided to limit result to training properties of someone else and by extending results cases domain has developed it in practice to obtain any kind of patent, profit and service. Such reputation is justifiable under shadow of differential and strict penal policy. Because it can in practice include more extensive behaviors and more offenders.

CONCLUSION

Development of information technology and electronic revolution encompasses all aspect of social life as determinant phenomenon of current century. In area of laws and crimes despite of conducted attempts the cyber space is still uncontrolled, chaotic and lawless space that is almost accessible for all people. In term of penal aspect the quantitative and qualitative differentiation of digital crimes comparing with conventional crimes challenges seriously the efficiency of usual penal system. In such manner that expert of rights and law and policy maker of this area have to contemplate and make new decision. The fundamental point in the area of punishment law and penal policy is quantitative and qualitative differences of cybercrime with real world. Speed, diversity, ease of commit, internationality, anonymity is among these differentiation. Ever-increasing dependency of economic, industrial, service and cultural infrastructures from one side and vulnerability of these infrastructures due to extensive development of cybercrimes and expansive dangers that address these development to mentioned infrastructures from other side necessitate building special penal policy in various aspect of control, management, prevention.

Present paper tried to examine differential approach of penal rights toward cybercrimes from viewpoint of general theories of punishment law. Main concentration of this reseach was on the fact that alongside with other special

strategies that should be taken against virtual world crimes one should clarify and make a differential penal approach. For taking such effective and efficient penal policy due to particular differentiation of such crimes it should define crimes, penal responsibility and punishment determination in a different manner so as to its inhibitions and preventive effect be fostered. In this paper one has attempted to explore and analyze some important aspect of differential penal approach.

REFERENCES

[1] A. S. Egger, Linkage Blindness: A systemic Myopia, in 8 seral murder: an Elusive phenomenon, 1990.

[2] W. S. Brenner, "Toward a criminal law for cyber space: distributed Security," *Journal of Science and Technology Law,* vol. 10, 2005.

[3] R. J. Vaca, Computer forensics, computer crime Scene Investigation, Chorles River Media, 2002.

[4] B. Stuart, Beyond our control? confrontg the limits of our Legal system in the Age of cyber space, the MIT Press, Cambrigde, Massachusette London, 2001.

[5] E. Hassanbeigi, law and security in cyberspace, cultural institue of international study of contemporary tools, Tehran, 2004.

[6] D. D. Markus, "Criminal law policing possession: The war on crime and the end of criminal law: computer crime-leglative proposal and explanatory memorandum," *The Journal ofcriminal Law & criminology,* vol. 91, no. 4, 2001.

[7] M. H. Deziani, "computer crime, chapter two, computer crime in terms of penal rights," *Journal if informatic,* p. 62, 1996.

[8] A. Javanjaffari, "cyber crime and differential approach of penal rights," *the Journal knowledge and development,* no. 34, 2010.

[9] R. Cooter and T. Ulen, Law and Economic, Harper Collins Publisher.

[10] M. Grayeli, "examining forgery and sabotage in computer system," *Journal of legal teachings,* no. 13, 2010.

[11] "informatic supreme councel secretariat, Iran bidget and planning organization," *the Journal of international criminal policies of United Nations,* 1997.

[12] K. K. Neal, "Criminal law in cyber space," www.nealkatyal.com.

[13] M. Fazli, "sabotage and disturbance in data of computer systems," in *series of articles of first conference of information technology right, the center of judiciary strategic and development of judiciary power*, Tehran, 2004.