Journal of Business and Social Science Review
Issue: Vol. 3; No.1; January 2022 (pp.21-27)
ISSN 2690-0866(Print) 2690-0874 (Online)
Website: www.jbssrnet.com
E-mail: editor@jbssrnet.com
Doi: 10.48150/jbssr.v3no1.2022.a2

Challenges Denial of Access to Legal and Penal Systems in Iran

Amin Amirian Farsani
Assistant Professor of Law
Shahid Ashrafi Esfahani University

Abstract:

Data associated with new human life is amazing، because correct operation of computer and telecommunications systems have highly effective and important role in the life of citizens and the Community is not possible without it, and it makes people more careful attention to computer security and to protect from their data and systems. Since the annual, number of users and organizations pay much money to the security of their data and systems, Impaired and to protect their data from access. Then it is necessary that penal system support from these individuals and organizations, move in line with this criminal is actions implement and apply Supplier, criminal and restorative appropriate criminal sanctions, and to protect from the De jure of missing of oppressed and protect the rights of society to a fair trial

Keywords: data**,** system**,** Denial, criminal law, security cyber

Introduction

Todays' life of human societies surprisingly is associated to the data, because precise performance of computer and telecommunication sites that has an affective and specifying role in the style and method of citizens' life is not possible without awareness about them and this causes people to pay attention to computer security to protect their data and sites. Computer security is a branch of information technology (IT) that is responsible for security and secure maintenance of data and information.

Protection, support and maintenance of computer data, important information, sensitive programs, necessary software and whatever is important in the secondary memory of the computer is called computer security. Generally, security contains three parts that are privacy, integrity and accessibility. It means that determination and guarantee of a network or secure system should result in the three stated purposes (Andoras, 1997, p. 45).

One of these three main and fundamental principles of computer security is accessibility that after principles of privacy and integrity is situated in the third place. As users and organizations annually pay heavy prices for security of data and their sites to prevent disruption and misapplication of data that endangers their accessibility spends some money; therefore, it is necessary to support victims by finding the crime and punishing the criminal.

Statement of the problem

Todays' life of human societies is connected to the data and information surprisingly, because appropriate performance of computer and telecommunication sites that plays an influential role in the style and pattern of citizen's life is not possible without deep understanding of these issues and this causes people to pay attention to computer security and to protect their data and sites.

Based on the least right of access every program and user that access to the system should use the least access limitations for completion of duties. Generally every system contains different parts that most of them require a set of basic accessibilities, but small numbers of these parts require higher accessibility than others that it is tolled these parts will be applied with promoted accessibility right. Programs that are related to these components will be marked and other programs that have no right of high access should not be signed (based on the law ENV00-J).

Computer security is a branch of Information technology that is responsible for security and maintenance of data and information. Protection, support and maintenance of computer data, important information, sensitive programs, necessary software and whatever is important in the secondary memory of the computer is called computer security. Generally, security contains three parts that are privacy, integrity and accessibility. It means that determination and guarantee of a network or secure system should result in the three stated purposes (Jalali Farahani, p. 2009, p. 12).

One of these three main and fundamental principles of computer security is accessibility that after principles of privacy and integrity is situated in the third place. As users and organizations annually pay heavy prices for security of data and their sites to prevent disruption and misapplication of data that endangers their accessibility spends some money; therefore, it is necessary to support victims by finding the crime and punishing the criminal (Aalipor, 2011, p. 223).

Denial of access has a direct and close relationship to the crime of computer disruption and even cyber terrorism, because subject of crime and criminal results occurred on data in the site and we can say that the crime of denial is one of the specific forms of disruption crime that has an absolute relationship to general and specific disruption (Fazli, 2004, p. 7).

A traditional and old attitude states that government is the owner of information and government is free to accept or not and is not obliged to be responsive. Therefore, the government idea in any conditions can deny people's access to the data and is not required to be responsive, but regarding civil responsibility prediction for government it should be specified that whether government is still criminal for civil responsibility or not? (Khoram Abadi, 2012, p.70).

Research objectives:

Main objectives

1. Introducing the crime of denial of accessibility to the data and site in Iran's penal code
2. Finding the methods of the crime of denial of access to the data and site

Secondary objectives

1. Introducing the cyber security gap
2. Introducing cyber criminals
3. Specifying the position of cyber criminals in the laws of computer crimes

Theoretical framework of the research

Theoretical framework of this study is derived from criminology and cyber security in the realm of IT and in discussions about cyber security computer data and sites are posed, spatially in the case of computer crimes and crimes against totality and precision of data and computer and telecommunication different theories and ideas are not considered, though in the conferences of analyzing legal dimensions of IT there are different ideas and discussions about supporting data and access of allowed individuals to them, but ideas did not result in a correct procedure (Khoram Abadi, 2004, p. 95). In the case of computer threats there were discussions about the rights of IT and a set of articles dealing with supporting data and computer sites was posed (Aalipor, 2009, p.82).

In discussions about criminology of cyber crimes in which referred to criminology of white collar crime or phosphoric criminals there are different ideas about their application in the case of ideas and suggestions regarding their application about computer crime terminologies that were posed and analyzed. In addition, the entire hypothesis, knowledge, properties, reports and information are called data. For registering and common understanding of every reality and phenomenon its specific signs were used. At first they are in the form of image and then the process of their evolution helping words, numbers and signs or a compound of them can be registered. Numbers, words, and signs that originate from common understanding and perception of human being or computers is called data (Jalali, 2005, p. 33). Data may not have anything in nature; because data are a set of 0 and 1 consequences that are result of symbols of realities, information or concepts somehow to have capability of processing in a computer system to be able to process them precisely to have a correct performance to result in application stage (Jai et al, 2004, p. 52). After different ideas and suggestions a computer site as follow was analyzed: a category or set of objectives that are relevant or irrelevant that follow some specific purposes so that they form a complex unit, or in another words every computer system that has the capacity of computer data processing are used for denial of access and site (Najafi, 1388, p. 28).

Review of the related literature

Searching for studies in this domain there was no book or thesis in this regard. Accordingly there was an article and a thesis that referred to the similar issues.

In the thesis "cyber terrorism" after dealing with discourse, classifying different types of discourse and expressing the policy of legal and criminal of Islamic Republic of Iran for terrorism specially cyber terrorism does cyber disruption. Cyber disruption in this thesis is a coverage concept with wastage of the data, information distortion, and fraud in the behalf of the domain or range and so on. Also, it should be specified that in this thesis the disruption crimes and denial of access is considered as a basis for cyber terrorism not as an independent crime. For this reason, the principles of composing crimes are not specified in detail (Pakzad, 2009, p. 82).

In the book "jurisprudence and legal analysis of computer crimes" authors dealt with jurisprudence and history of computer crimes. This book represents jurisprudence and history of computer crimes. This book represents crimes in electronic trade law relying on international laws. Also it should be considered that publication of this book is prior to the law of computer crimes (Bay- Por Ghahremani, 2009, p. 82).

In the article "disrupting computer software with a new attitude to the crime of criminal destruction, after representing principles of traditional destruction crime, according to the legal bill of computer crime does disruption in the data and computer sites. He considered, in fact, data equal to computer software and provided financial features for these computer software, while not only in the computer crime laws, but also in the criminal bill of computer crime punishments there is not such limitation. Also it should be considered that there are principle changes in the bill of computer crime law (Nami, 2007, p. 58). In the article of disruption and destruction of data and computer systems that were analyzed in the first conference of studying legal dimensions of IT, the disruption crime or data destruction are nor separated from computer crimes and they believe that always there has been destruction and now they are applied on data. While we should say that the basis of computer crimes is purity of cyber subjects. In fact crimes are considered as pure computer crimes that happened in the cyber space and in the crime disruption and data destruction are the same. Another point is that this article is written based on international conventions and laws (Fazli, 2010, p. 42).

In the book "computer crimes" after representing the quality of computer crimes and related reports the general features of cyberspace and cyber criminals were studied. As cyber terrorism danger threats information society and just represents some observations in this regard and finally speaks about cyber police, hackers and crackers. This book has no sufficient attention to laws and international conventions that supervise computer crimes (Jinadi, 2003, p. 35).

In the law of IT and communication (compilation of articles)

Security of the cyberspace that is one of the main items of IT, both security of the data and users and people by means of filtering dangerous and abnormal information is achieved and cyber security will have a close relationship to national security.

He concluded that national security in the cyberspace depends on information security and until information security is not corrupted national security will not be threaten (Aalipor, 2009, p. 225). Researcher tries to analyze the crime of denial of access.

Methodology

The methodology of this study is descriptive and analysis of the materials related to the denial of access to the data and site in which compilation of information is done using library method. In other words it refers to documented references and library books, note taking and using internet references. This study in which guarantees the issues and subjects and also their evaluation and validity is done using library method of research. The tools of analysis in this study are based on using the logical method and using logical inferences and applying basic legal principles.

Analysis of denial of access

Principles of the crime denial of access to the data and sites:

Legal principle: the first and main element for introducing every crime is legal element that in the article 36 of constitution states that "decree to punishment and executing it only by means of the just court and by means of law." In the Islamic penal code 2013, article 12 called it a separate article and in this respect at first we should introduce the legal element of every crime (Bakhshizadeh, 2012, p. 34).

In the law of Iran's computer crimes denial of access to the data and site in the article 10 of computer crimes (article 738 of the Islamic Penal Code) is anticipated and denial of servicing or stopping data result in disruption in the performance of the system that is criminology that is the case of article 9 of the law (Elahi Manesh, Sedrah Neshin, 2012, p. 135).

As denial of access for the right of access to the data is of the initial principles of data and information security is separated from another principle, but as denial of access causes lack of natural function and precise data, site and network, they are documented under cases of cyber disruption (Aalipor, 2011, p. 220).

Therefore, the crime of denial of access to the data and site in article 10 of the law of the computer crimes (738 Islamic Penal Code) is referred to that is as follow:

Every one illegally with applications such as hiding data, changing passwords cause denial of legal individuals to the data or sites and these criminals will be punished to 5000000 rial to 20000000 rial or they will be punished to both punishment items.

According to this article that is about crime of denial of access to the data and site, we should say that criminology and punishment of this crime is specified in a separate article. Though it is discussed in the discussions related to the computer crimes; therefore, we should not forget in issue that in the conventions of cyberspace crime 2001 in Budapest this crime is not specified separately in a specific article and just Iran's legal principle to it specifies that though in Iran the third category of the crimes are called crimes against access to the data and site in the privacy and totality of data and sites is not predicted, but crime of denial of access to the data and site is discussed and subjected to criminology in another article.

Material principle:

What can be discussed in the material principle is that every crime necessarily has one material element that accordingly we conclude that research about crime refers to representation of external side effects that is the willing of doing crime that until it is representation of some forms like action and stopping action is not achieved, no crime will arise (Goldozian, 2005, p. 153).

In the material principle the subject of crime and behavior is analyzed that in this domain at first we deal with analyzing the subject and dimension of behavior.

Crime subject:

The subject of crime is something that legislation support it as a value or in another words it is something that is opted to a criminal behavior. In the crime of denial of access to the data and site what is respected by legislation is data and site and against conversion of cyber crimes that denial or stopping is just predicted to data it is more interesting that along with crime disruption in the data is discussed. In Iran, however, according to article 10 of computer crime both data and site are supported, but we should see that whether services of site application or in another words denial of access to the internet or communicative services are inserted in this article or not?

Also this issue should be reminded that what is effective in denial of access is prominent is denial of site services that one may have access to his computer site, but my not access to it because of others denial. In fact access to the services is not important but access to the services is important and using logical interpretations we should say that predicted behaviors like denial of access and denial of services are both important (Aalipor, 2011, p. 230).

Accessibility services:

Accessibility services are those services that are offered by individuals that offer internet services for access of individuals to the data and information in the internet network and receiving and sending information. Accessibility services are the most principle services that are offered by providers of internet services and daily millions of individuals in the world are connected to the information in the internet network and enable them to sending their information (Fazli, 2010, p. 96).

Providers of Internet services in accessibility services as “mere conduit, gateway and passage way” acts for users connection to the internet that using them and passing through computer equipment reaches to them and consequently will be transferred (Chalender., 2003, p. 57).

Behavior:

In the crime denial of access to the data and site what is crystal clear is denial of access that respecting the approaches of the site means user denial of application of internet or using the same system (janczewk L.etall,op.cit,p.85). In fact, multiuser operating system is the purpose of attacks such as denial of servicing, so that one user can by means of deviation and damaging resources inefficient (Aalipor, 2011, p. 230).

The patterns of doing crime of denial of access

A. Computer Viruses:
Viruses have damaging consequences (but sometimes they are not dangerous) for example some of the viruses can damage the hard disk of computers or occupy a memory that for other reasons they need programs. Virouses are dangerious when before controlling them, they are distributed. Therefore, as it is not possible to prevent their development, they create a great deal of damages to the data and sites and sometimes they deny access to the data and during the time that they are used thousands of computer viruses damage data and information of individuals or causes disruption in the application of the computer systems that we can refer to viruses of Melissa, Explore Zip, Chernobyl, I Love You. Pakistani mind and Mic Anj that are denial of access (Fazli, 2004, p. 152).
B. Trojans: in the computer sciences, however, Trojan horse is similar to the legendary horses and it is a program that is apparently beneficial and suitable. But in nature it covers damaging and disrupting programs (Cyber Terrorism in the Context of globalization). Computer Trojan horses have different types that discussing about them we can refer to then as remote administration Trojans, password Trojans, and destructive Trojans (Bay, Porghahremani, 2009, p. 166).
C. Computer worms: most of the people mistaken computer worms for viruses, because both of them damage computer or site and can have destructive affects like files and cleaning the entire disk. Worms’s experts are a subset of viruses and sometimes the term virus is used to refer to them (Mantin, p. 54).
The main difference between virus and worm is that worms are active in the network, but activity of the virus depends of reproduction or physical copy. In other words, viruses are content to stay in the system to damage one file after another but worms are searching for new borders.
D. Attacks of denial of service DOS and distributed denial of service DDOS: DOS attacks are to deprive people from access to the computer systems and when these attacks happen in the network they are called DDOS attacks. In fact, the main reason for representing danger of these attacks is limited nature of system resources and computer systems like band width with ability of processing and possibility of saving them (Fazli, 2004, p. 185).

Mental (spiritual) principle: for a crime it is not sufficient to reject orders and areas of legislation. Reality of the crime depends on this issue that disregarding orders of legislator entails punishment and is guilt and the main condition of guilt is that refusal of punishment law to refer to the act of someone who is probably guilty (Baheri, 2005, p. 264). It seems that crime of denial of access to the data and site is an intentional crime that needs general and specific bad intention and ith these cases criminology in the unintentional states in the case of sensitive and necessiry sites are not acceptable and it is necessary to consider the general bad intention to follow the criminal (Elahi Manesh, Sedrah Neshin, 2012, p. 66).

General features of the crime of denial of access:

A. Denial of access should be illegal. As the illegal is a common term for most of the computer crimes and therefore in the law of computer crimes they are inserted several times, one should say that in the article in article 738 beside the condition of illegality of access we deal with legality of those who have access to the data and site. Legal individuals are legal owners and people who by means of law or by means of just judge have access to the data or site (Aalipor, 2011, p. 228).
B. The crime of denial of access to the data and site is a pure computer crime. “ Interpreting actions like hiding data , changing keywords and cods” that are used in article 738 shows that denial of access like cyber disruption is pure computer crime and happens in the cyber environment. Therefore, if by cutting off electricity or locking the door of the place that site is located in or hiding the password of company or firing papers of the passwords are to prevent the user or owner to access to the site or any other physical activities are subject to article 738 (Aalipor, 2011, p. 228).

Research hypotheses:

1. Access to the data and site needs criminal support.
2. Access to the data and site with crimes of disruption and terrorism has general and absoulute relationship.

Conclusion:

Today's life of human societies surprisingly connected to the data, because correct performance of computer and tellecomunication sites has an effective and determining role in the style and patern of citizen's life so that without it life is not possible and causes that people more pay attention to the computer security to support data and sites. Computer security is a branch of IT that is responsible for security and maintaining the data, important information, sensitive programs, necessary softwares and whatever exist in computers secondary memories are called computer security. In a general sense security contains three parts that are: privacy, integration, and accessibly. It means that specification and guarantee of one network or system should result in three purposes. As e-mail service is changed to the necessary and applied tool in different personal, economical and social parts and great parts of individuals information in these emails are saved preventing access to them result in different material and spiritual damages.

As the right of access to the data and site is one of the rights of individuals therefore, we can say that in no condition we can corrupt the right of individuals, but in some conditions these will be isolated with legal allowance.

They should see peoples information or preserve data of some individuals. But if someone limit or deny access of people to informationthen it is not possible even with legal allawence. Therefore we should say that denial of access to the data and site is a new crime that should be considered by legislation and they should apply preventive olicies of crimes after crime.

Suggestions

1. FTA police with help of governmental organizations and with an appropriate grounding for organizations in the case of decreasing security advantures needs holding conferences and education in the group form.
2. Legislature with help of judiciary system tried to predict different punishments in the case of different crimials to prevent repetation of aafective crimes.
3. Judges of criminal courts and spacialy judges of courts of cyber crimes did complementary punishment in denial of access to the data and site to prevent individuals from the right of having computer or they should be restricted.
4. Restricting the rate of using allowed users and specific rate of access right that more than the same thing needs administrative regulations and desiplains for organization that requires discharging them from servicing.
5. Usage of FTA police with cooperation of broadcasting for alerting and offering educational points and security advatures in the form of doucumentry film or specific brochures.
6. Cooperation of FTA police with schools and education for increasing the level of students and family in the realm of cyber cecurity and introducing the methods of resistance and getting out of crisis in behalf of the rxpertss in the realm of cyber crimes
7. Usage of FTA police from cyber criminals and creakers in the process of weak introduction of systems and increasing security to prevent illegal enterance of individuals to the data and computer sites.

Resources

Elahi Manesh, M. Sadreh Neshin, A. (2012) Computer Crime Law Mhshay , Tehran; Majd publication. First edition.

Andrvras , Tannin Baum (1997) Computer Networks (translated by Mohammad Qudsi) Supreme Council of Tehran Anphormatic

Baheri , M. (2005), the attitude of the general criminal law , Tehran , Majd Publication, second edition

Bai H and Porqhrmani, B. (2009) Investigating Computer Crime Law jurisprudence , Tehran , Institute of Islamic Sciences and Culture Publication, first edition.

Bakhshizadeh , A .(2012) New developments in the approach of the Penal Code Act , Tehran, Cheraghe Danesh Publication, First Edition.

Pakzad , B. (2011) , cyber terrorism , a new threat to national security , First edition, Tehran , publication of the office of developing science production

Jalali , AA , (2003) Electronic City , Tehran , Iran University of Science and Technology publication , First Edition

Jalali Farahani , AH (..) cyber terrorism , Journal of Law and Jurisprudence , Third Year , No. 10

Khodagholi, Z. (2004) Computer Crimes , Tehran publication of Arian First edition.

Khorramabadi, A. (2012) criminal responsibility of Internet service providers , Isfahan, Dadyar Publications, First Edition.

Khorramabad , A.(2004) History , Definition and Classification of Computer Crime Law Set Conference on Information Technology Evaluation - Department of Justice Legal and judicial development

Aalipour , H.(2011) Criminal Law Information Technology , Tehran, Khorsand Publication , First edition

Aalipour , H. (2009) , safety and security in cyberspace : Computer threats against national security , law, information and communication technology (Proceedings) , compiled by Amir Hossein Jalali Farahani , Tehran , Islamic Republic of Iran's official newspaper publication

Alipour , H. (200) , Computer Crime , Computer Crime Masters Course notes , Department of Administrative Sciences and Economics, Department of Law

Fazli , M.(2010) Criminal responsibility in cyberspace Tehran , Khorsand publication

Fazli , M. (12004). The destruction and disruption of computer data and systems , Proceedings of the conference on legal aspects of information technology , compiler of the Judiciary , Vice President for Legal and judicial development , printing, Tehran , Salsabeel Publication

Goldouzian , I.(2005) required by the general criminal law , Thranantsharat amount 12 Edition Najafi Abrandi Abadi , A.(2009) , the new penology - New Criminology : An Introduction to Criminal Brsyast Khtrmdar management , science news articles of crime , under Ali Hussain Najafi Abrndabady , first edition, Tehran , Mizan publication Talking with B. Razavi Fared, Professor of Allameh Tabatabai University , November 2012

Chalender, Jennifer A.**(2003)**; **((**Security in cyberspace**))**: Combating in Distribute Denial of Service Attacs, Law & Technology Journal, University of Oattwa

Mantin-Wasik-**(1991)**((crime and computer))Oxford Publications

http://www.nosa.com/nosaweb/Products/Simorgh/InnerPages.aspx%3FPageId%3D475