Cumhuriyet Üniversitesi Fen Fakültesi
Fen Bilimleri Dergisi (CFD), Cilt:36, No: 3 Özel Sayı (2015)
ISSN: 1300-1949

Cumhuriyet University Faculty of Science
Science Journal (CSJ), Vol. 36, No: 3 Special Issue (2015)
ISSN: 1300-1949

Criminal protection of Privacy in cyberspace

Ameneh MIRHOSEINIYAN

Graduate student of Criminal Law and Criminology, Islamic Azad University of yazd, iran

Received: 01.02.2015; Accepted: 05.05.2015

Abstract. Criminal protection ought to be sought by criminalization and the deterrent power of criminal reaction to the crime known to be the most basic form of criminal protection. This study aims to investigate the basics and notions of criminal protection in privacy. From the beginning of mankind's life, security has been one of his chief concerns. Nowadays, as the internet and other networks are growing constantly in our country, the need to provide security in cyberspace can be felt more than before. It is sensible reaction existing in terms of fear for damaging the moral and social principles, and of lack of mental and cultural security owing to pernicious and morally corrupted information on the internet and cyberspace on the grounds that each society has its own informational frameworks. It is natural that information trespassing these borders and lines can be dangerous to the security and moral health of society. Although there are some upsides in regard to the global networks, misuse of networks has jeopardized privacy of individuals. On the one hand, people rely on the right to gain the advantages of private space on account of personal needs. On the other hand, they must recognize this right for others because of the necessity of communal life. However, recently, with ever-increasing growth of media tools and widespread use of internet, this right has been presented to be one of the most formidable challenges of human rights. Concerning the fact that users are unknown and internet is very accessible, invasion to privacy has been on the rise, and this propelled experts and politicians to advocate the privacy.

Key words: privacy, cyberspace, criminal protection

1. INTRODUCTION

Privacy is one of those concepts that are very accessible and each person can grasp but thorough and comprehensive possible cannot be put forward. In this respect, this poses a dire problem and paradox in many cases. Articles 22, 23, 25 in constitution of Islamic Republic of Iran forbid any invasion to privacy and private information. Besides, the regular laws protect the privacy, individual honor and deals with how to punish individuals who engage in impermissible activities in audio and visual fields; for example, act 640 of Islamic punishment law has anticipated prison and fine for criminals. In computer criminal law, the invasion of privacy has been criminalized patently in acts 2, 14, 15, 16. Cyberspace is a big community in which millions of computers and theirs users are interconnected to each other. Seemingly, the dominance the computer in daily lives provides the ground for creating norms and mores on the internet. Cyberspace is exotic space, where people introduce themselves by means of talking and no one knows another really. Persons gather together via international networks in these spaces and crime is one of the social phenomena; therefore when people muster and crime accompanies them, it is possible to speculate that this area like other social elements cannot be safe and sound from this flexible and inseparable part of society called crime. (Supreme committee of information, 52:72). By and large, what comes under the heading of cybercrimes consists of two groups: the first group is crimes that exist in physical world as well and cyberspace can facilitate the crime by providing them with necessary tools and without changing its basics. The crimes in this area are very vast and they includes a wide range of crimes from crime against national security or international ones such as terrorist activities to offences against people and their properties. One example of this type is seditious speech in cyberspace. But another group of cyberspace is misuses unique to this space that can be carried

*Corresponding author. *Email address: Ameneh MIRHOSEINIYAN*

Special Issue: The Second National Conference on Applied Research in Science and Technology

http://dergi.cumhuriyet.edu.tr/cumuscij

out in physical space. Crimes such as impermissible access to data and systems or spreading pernicious programs such as virus can be committed only cyberspace and for this reason they are called pure cybercrime. (Casey, 2001:8) Nowadays, humans are looking for a chance to escape from pollutions, crowd places and exhaustion and to find exuberance and liveliness in their lives. IT in cyberspace is moving toward proving more comfort, easier interaction and constructive communications in society, and to do better services for citizens of a society (Farahani Jam: 1385). On the grounds that this study aims to investigate the criminal protection of privacy in cyberspace, researcher is going to illustrate the relevant factors and problems.

2. PRIVACY AND CONCEPT OF PROTECTION

Acceptance of privacy as human right has roots in history. In Bible, Jewish principles and in ancient China there was some immunity in this matter. Some authors dates it back to ancient Rome and Greece attributes its origin to the necessity of ownership right to assets. In 1361, an English judge issued an order for arrest for those who looked at people's house on the sly and eavesdropped. When theory of privacy and the request for protection has been put forward for the first time, the driving force behind it was misuse of press and journalists' interference in privacy of people (www. Maavan news.ir).

Protection signifies support and defense of someone and necessary action to be taken to defend the rights of the victim and to uphold his violated rights. "Keifar" literary means the reward for good or bad actions and retribution (Moeen, 1384, 963) and is synonym for punishment. The concept of punishment has a long historical background and it is said that "we can discuss it as long as the mankind has lived." (Nourbaha, 1378, 387). Punishment is the result of anti-social action. But imposing this punishment pursues a moral and utilitarian goal at the same time (Boulk, 1382, 29). Although privacy is one of the most tangible and useful right for each person but experts could not agree on one unique definition. In the 1990s, one of the judges in supreme court of the USA named Louis Brandis has put forward this problem for the first time in an article named "immunity right to privacy" and defined as a right for being alone (Mohseni, 1389, 250). Some try to connect this concept to the right in taking advantage of independence, and whether or how to make their own information visible for others. "Westin" offers an useful definition for privacy: "privacy is the right of people, groups and institutions to determine how long and to what degree they want to transfer their own information." (Westin, 1967, 7). Some consider this right to be right of supervision for disclosing their own information and others perceives it as the right to hide their truth of life from others (ibid). Committee called Calcutt in the UK accepts this definition as the legal one: "people's right for protection against entering and interfering social life without permission by means of direct physical tools or by spreading information" (Calcutt committee, 1990). Helen Nisbam uses right to privacy rather than privacy in which people can be free from the exact and rigorous inspection or perhaps blame for their own personal affair (Ansari, 1390, 52). Privacy designates the right to be alone; the right of limited access of others to humans and the ability to create barriers against unintentional accesses to humans; the right to hide some of your affairs from others; the right to control your personal information; the right to support to personality and human esteem; the right to have human's friendliness. (Foord, 2002, 1092)

2.1. The violation of privacy and its examples

The violation of privacy is to enter and have impermissible access to data and private information in cyberspace. Because this cyberspace is vulnerable and needs the support of lawmakers, it is necessary that, in the first place, the examples of violation of privacy should be illuminated and then solutions are provided. It is possible to divide privacy into four different and separate areas:

1. The information privacy that includes passing some laws that protects the information such as financial information, medicinal and so on. This is also known as protection of information.
2. The physical privacy is the protection of people body in the face of genetic experiments and so on.
3. The communication privacy is the protection of electronic emails, telephones, posts and other forms of communication.
4. Spacial privacy is the sum of limitations and supervisions in work space, lives and public places. (Ansari, 1390)

There are also 10 examples of violation to these privacies in international congress of lawyer in Stockholm held in 1967:

1. Inference in private lives
2. Violation of the physical and mental entirety of a person and imposing moral and spiritual limitations.
3. Violation of honor and reputation
4. Wrong interpretation of statements and actions
5. Using persons' name, identity or picture for commercial purposes
6. Disclosing annoying things about persons' lives
7. Doing espionage and spying on other people's lives
8. Confiscation and inspection of private correspondence
9. Misusing of written or spoken correspondence
10. Disclosing profession and vocational information

Therefore, it is enough to put emphasis on the individuality of people in order to play up the role of privacy. Lack of privacy for an individual is the sign of destruction of his individuality because there would be no consciousness at that time. Destroying persons' individuality leaves humans' face with nothing except puppy. (www.maavanews.ir)

2.2. Privacy in Iran

According to some verses in Quran such as verses 27 and 28 of Noor surah pointing out the spacial privacy and also per to the some stories in Islam, the importance of no interference in privacy is very crystal clear in Islamic Republic of Iran. Imam Khomeini, who has followed all the rules of Islam, protected people's privacy by issuing a 8 article- order to Legislative power and other executive organizations enforcing Islam rules in 61/9/24. In this order, it is crime and therefore forbidden to enter peoples' homes or their work place, eavesdropping to tape, interfering in peoples' secret life and disclosing it or recording peoples' sound under the name of discovering crime. In laws 22, 23, 25 of constitution it is possible to find these rights as well. Law 22 states that "life, honor, property, rights and home of people is immune from people unless law orders such." Law 23 has banned the inquisition and law 25 states this problem that "inspection, not delivering the mails, recording and disclosing the phone talks or telecommunication, censorship, eavesdropping and any kind of inspection is forbidden with the exception that law orders." However, the necessity of making some especial laws to protect the privacy is felt because laws deals with general issues and details are on the shoulder of regular rules in which the limitations and its aspects and its punishments are paid attention. The scheme of protecting privacy published 85/4/8 can be considered a bonus. In this scheme, the privacy of body, home, work place, private information, and private information in media activities has been paid attention and so are the consequences. One of the topics relevant to this study is privacy and the internet communication in article, 70. In article 65, "bugging, recording, saving, or any other kinds of interception of private communication on the internet without their permission is not allowed." Article 65 also states that ISP must take into consideration any technical and bureaucratic to provide security and service. (Mohseni, 1389)

3. PRIVACY IN INTERNATIONAL DOCUMENTS

The right of privacy is stated clearly in international laws. Following the human right declaration and its acceptance in 1948 and article 12 that directly deals with the topic of privacy, similar conditions in civil and law international contract and Europe Convention regarding the human rights and other conventions and regional treatments are stipulated. Human right declaration in article 3 states, "Each person has the right to live, to be free and to have personal security." And also article 12 states, "there must be no arbitrary interference in peoples' private lives, home and their correspondence or someone's honor reputation has ever been reviled. Having the right to legal protection in the face of these violations is everyone rights. The European committee in resolution about privacy stated that privacy is right to have the life with whatever interest people have and there must be the least interference in peoples' lives. Lawyers' conference on protecting privacy held in Norway stated in its second article of its declaration that "the right of privacy is one in which someone can be alone in his life and live the way she likes and there must be the least interference in peoples' lives." In Islamic human rights passed 1411 in Cairo also referred to this right of privacy, "each human has the right to have independence in life. Any kind of espionage or supervision or reviling honor is not suitable and he must be protected against any oppressive violation." Committee of supreme leaders heeds the right of privacy in their declaration about the informational society passed in 2003. article 35 of this declaration states, "reinforcing the safe framework such as the security of information and the network, credit guarantee, protection of privacy and protection of consumer are the prerequisites for creating informational society and creating trust among the users of IT. Article 58 also highlights human rights and basic freedoms like protection of privacy in the use of IT. (Mohseni. 1389)

4. THE PRINCIPLES OF PRIVACY PROTECTION

The right of privacy is the most important right that is in tie with human esteem and its goal is to edify human namely, respecting material and spiritual aspects of humans. Privacy creates the necessary space for the growth and development of individuals and prevents the process of commodification of humans. Furthermore privacy is one of the foundations of civil society raising the possibility of existence of private organization. (Ansari, 1383, 2)

4.1. Religious principles

The necessity of protection of privacy and lack of interference in private lives of people is one of the didactic basics of Islam and nowadays this notion as of the most significant values has been protected in Human Rights of any regime. With this in mind, Islam pinpointed the protection of privacy and forbidden its violation 1400 years ago and in various verses of Quran, the necessity of privacy protection has been highlighted. Prophet Mohammad Sonat and the faithful way of life are replete with these respects to privacy. The clearest example is verses 27 and 28 of Noor surah in Quran that protects privacy. Quran says, "oh the faithful, d not enter houses that are not yours unless you are familiar and say hello." it can be understood from these verses entrance to privacy needs permission and interference in others' private lives is forbidden and when prophet Mohammad intended to enter someone's house, he did not stand in front of the house so that he would not see the inside. (Jafari, 1385, 46) Place and importance of privacy has been studied in Islamic Constitutional law and this result has been achieved that in this system of law roots of violation of privacy has been disapproved and in fact this has taken heed of privacy fundamentally. In this respect, various verses and stories (Revayat) in Islam has been referred to and the most important examples of violation of privacy are inspection, interference, backbiting, defamation, bugging, and entrance to house without permission, corruption and betrayal. Although privacy has not been protected very explicitly but law167 of constitution and article 3 of code of civil procedure has obliged the judge to issue a decree by referring to Islamic credible sources or credible Fatwah in case the law is not effective. Therefore it is possible to

claim that the topic of protection of privacy in Islam sources has entered Iran constitutional law indirectly and it can be inferred and stipulated in legislations. Article 167 in constitution states that "judge must endeavor to find the decree in written laws and if not, he should issue the decree using credible Islamic sources or credible Fatawah and the judge should not evade the problem of issuing the decree under the pretext of silence, violation" (Ansari, law of privacy, Samt Pub, 1390). In article 3 in code of criminal procedure passed 1379/1/28, it is stated, "judges in courts are obliged to issue the suitable decree based on the laws. In case law are not clear or they are paradoxical or even there is no offered statement about it, judge must issue a decree based on Islamic credible sources or Fatawah or laws that are not different from the Islam rules and they should not evade it on the pretext of silence or conflict of laws "there is no conflict in view about protecting privacy." (Asani, 1384, 100)

4.2. Prohibition of Bugging

Islam is replete with pieces of advice about protecting privacy of persons by means of looking. According to the Islam principles, no one can open door to someone's house without his permission or to open the window. But if someone does this action, his neighbor can set a window or draw the curtain to put up barrier to block their views. It is recommended in Islam that doctors must not look at women's sexual organ when examining their body. Nowadays, sexual organs are a part of persons' privacy. (Ansari, 1390, 73)

4.3. Prohibition of Corruption and defamation

Islam has banned not only government but also thirst party people from entering privacy and has ordered humans not to disclose private affairs of people when hidden, they are far better. Prophet Mohammad has stated that someone who tries to spread corruption is like person who has done it. Prohibition of corruption is in tie with defamation and the necessity to hide others' mistakes and their weakness and is one inseparable part of human rights; this defends the humanity firmly and is barrier to human's action to mortify them. (Ansari, 1390, 73)

4.4. Prohibition of Spreading Corruption and defamation

Islam has banned not only government but also thirst party people from entering privacy and has ordered humans not to disclose private affairs of people when hidden, they are far better. Prophet Mohammad has stated that someone who tries to spread corruption is like person who has done it. Prohibition of corruption is in tie with defamation and the necessity to hide others' mistakes and is one inseparable part of human rights; this defends the humanity firmly and is barrier to human's action to mortify them. (Ansari, 1390, 73)

4.5. Prohibition of entering peoples' house without permission

Estinas means that on entering someone's house, people should introduce themselves and in case he remembered the person, he will invite that person on his own accord. Estizan is the act of getting permission from the landowner before entering. Estinas and Estizan are two necessary conditions for inspection peoples' house which is the necessary part of equitable criminal procedure. (Jalali Farahani, 1383, 8)

4.6. Principles of Human Rights

Nearly all the documents passed by international powers on human rights concentrate on this point that mankind should have rights and liberties protected in the way that is effective and governments are obliged to take necessary measures to protect individuals' rights. One of these rights is right to privacy. At international level, universal declaration of human rights in1948 in articles 3 and 12; international convention of civil and political rights in 1966, article 17; convention of Children rights in 1989, article 16; violation of privacy of people such as inspection and interference in their private life are banned. One these eights is the right to

privacy. Respect to private life in many international and regional human rights is highlighted. Article 17 of international treaty of political and civil rights deals with the right to privacy and has endeavored to follow universal declaration of human rights. This article states, "in private life, family, home or communications, nobody must mortify the honor of others and illegal damage to someone. Everyone has right to legal protection in the face of such damage." As it can be seen in this article, if the interference in peoples' privacy, family or communication is illegal or arbitrary , the committee of human rights that has been anticipated to supervise and coordinate the countries' performance in the convention, in the interpretation of the article and rights to privacy, has declared that protection of privacy is fairly necessary. The above committee has declared on the subject of law basis for the interference in privacy that every country should draw up some rules to protect the privacy before everything else unless some rules are stipulated in advance. Moreover, "law on the basis of entrance to privacy must be in close tie to rules, goals and objectives of the convention." Therefore, in one particular law, all the necessary and exact conditions in which the interference to privacy is permissible must be illustrated thoroughly. Article 8 of European convention of human rights states that:

1. Everybody has right to the privacy, family, home and communication
2. Governmental officials do not have any right to interfere in these rights unless it is according to law and it must be in the framework of democratic society for the national security, public health or economical welfare, prevention of chaos or protection of hygiene or morality or protection of laws or liberties of others". In addition, European authority of human rights has designated the exact meaning of "according to". The verdict clarifies that there must be a law in national rights of countries and the quality of law must be good. Therefore, interference in privacy can be carried out per to some national law. These laws are must be accessible to the people of the society in the way they are aware of these laws. The aforementioned laws must be drawn up with maximum clarity and exactness so that people can see the conditions in which the interference is permissible. (Khodagholi, 1382, 51)

5. EXAMPLES OF VIOLATIONS OF PRIVACY IN CYBERSPACE

This topic consists of three parts investigating the examples of violation of privacy. The first section deals with crimes relating to spiritual entirety and section two deals with crimes against assets and third one deals with crimes against public safety.

5.1. Cyberspace libel

"Touhin" is the infinitive meaning degrade, weaken and debase and as the gerund it means libels and insults (Moeen, Persian dictionary, ed 8, 1371). Touhin means degrade, debase and defame and as the gerund it means degrading and debasing. (Moeen, 408, 1371) libel crime is one of the crimes that is a part of spiritual prestige. Touhin is extracted from the root "Vahn" and it means weaken, degrade or debase. This word implies any kind of behavior, action, writing that can degrade someone ordinary and member of the public. In law terms, libel is used in its ordinary meaning." Libel that has been made on the internet is liable to be punished because it should be counted as a crime. Therefore, everyone who is wise, mature and free that insults and libels on the internet or do something accusing someone of something else forbidden, and if it is proved, then it is crime and it is punishable (Pad, 242, 1348). In Iran's laws and rules, some articles are dedicated to libel in general and others in particular. Article 16 of cyberspace crime states that anyone who changes or distorts someone else film, audio or picture by means on computer or communicative equipment or publish them intentionally the way it defames, he will be sentenced to 91 and two years prison or fine of 5 million to 40 million rial or both of these crimes. Note: if change or distortion is outrageous, felon will be punished with both of these sentences. Article 17 of cyberspace crimes stated that if anyone publish picture, private film or others' secrets without their permission and satisfaction using

computer or other communicative devices or make them accessible to others the way that it defames them, he will be sentenced to 91 and two years prison or fine of 5 million to 40 million rial or both of these crimes. (Fazli, 1388, 143)

5.2. Spreading lies

Spreading lies means reveal, disclose or state literally. (Moeen, 299, 1371) the meaning of spreading lie in law terms is to allege someone publicly in a way that it can be spread. As one thorough definition, it is possible that spreading lies can be defined as "spreading false news for the purpose of sedition or disturbing the public minds or officials." Spreading lies in cyberspace means spreading lies. The issue at hand is the security of people and individuals. Security is at stake when someone wants to harm someone else or to disturb people's minds or legal personality. Spreading lies is regular or common crime that in article 746 is referred to. But because internet is suitable space for spreading lies and on the grounds that there are some limitations and loopholes in traditional and old law, the criminalization of spreading lies in cyberspace is justifiable from the perspective of people. This crime in article 18 of cyberspace crime has been paid attention to. According to aforementioned article, "anyone spread lies by means of computer or communicative devices with the intention of damaging others or disturbing public mind or high rank officials or make them accessible to others or allege some false statements to a real or legal personality directly or indirectly or explicitly or implicitly, whether damage is done or not, he will be sentenced to 90 and 2 yeas prison. (Article 18 of cyberspace crime)

5.3. Tapping

Shonud (listening) is Persian word and its root is Shenidan and it means listening to any voice or sound. This is also equivalent to eavesdropping that has the meaning of listening to someone's private dialogue without their permission. Although no clear cut definition has not been suggested yet but notion and examples are determined to some extent and this notion has been used in its extensive meanings in laws as well. Bugging such as impermissible access arises from lack of satisfaction or legality of the transferring content. In addition, the condition of illegality is added to condition of approval. Cyberspace tapping consists of cases such as listening to others' phone talks, walki-talkie frequencies and the examples that exist on the internet. (Jalal Farahani, 1383, 15) the basics of this crime is article 2 of cyberspace crime (730) this crime is the same of violation to communication domain by means of traditional tapping and recording of private phone talks. Article two of cyberspace crime also refers to this crime. Article 2(article 730) states that everyone tapping the private transferring content in computer or communicative devices or electromagnetic or light waves will be sentenced to between 6 months and two years punishment or the fine of 10 million to 40 million or both of them at the same time. According to article 582 of Islamic punishment laws in1376, in case each janitor or office worker disclose any of the posts or private phone calls with the exception of cases law has permitted the opening or inspection or tapping, he will be sentenced to between 1 and 3 years or fine of 6 and 18 million rial. (Islamic punishment law)

5.4. Hoax call

Any sort of disturbance to others by means of hoax call (it is an example of disturbance). According to law, it is crime and the felon will be punished per to laws. According to article 641, whenever someone disturb by means of telephone or communicative devices, he will be sentenced to between one and six months in prison. (Jalal Farahani, 1383, 11)

5.5. Crimes against Properties

5.5.1. sabotage, vandalism and infiltration

Computer sabotage includes any sort of behavior destroying data completely or slightly or disrupts the performance of computer. The topic is computer data sabotage and this data must belong to someone else whether this is private or valuable or standard or it belongs to governmental, four kinds of conduct are predicted for this crime in article 8 of cyberspace crime such as deletion, sabotage, disrupting and making it unable to process. Two kinds of behavior of deletion and sabotage happen in connection to data itself and the rest of behavior happen in tie with performance and capability of data. All four kinds of behavior happen in cyberspace. This problem can be clarified with statement of that "computer or communicative devices" and the felonies must be cyberspace. In these law and rules there are some cases devoted to computer sabotage in general or particular. Article 8 of cyberspace of (736) state that "anyone deleting, sabotaging, disrupting or making it unable to process the data by means of computer or communicative devices will be sentenced to between 6 and 24 months or fine of between 10 and 40 million or both of them at the same time. Sabotaging designates the deletion the whole or some parts of something and disrupting means to create inability and frustration. Article 8 of cyberspace has predicted this crime. Article 8 (736) states that " anyone deleting, sabotaging, disrupting or making it unable to process the data of other computer or communicative devices will be sentenced between 6 and 24 months or fine of between 10 and 40 million or both of them at the same time. Disrupting means the act of entering, transferring, spreading, stopping the computer or communicative devices. The device might belong to real or legal personality or it might belong to governmental organizations. The disruption of governmental devices will increase the crime. In article 9 of cyberspace, two sorts of behavior are predicted; first is a kind of behavior that includes disrupting and sabotaging and second is sort of behavior that are in the first line of article and are accessing, transferring, spreading, deleting, sabotaging. In law and rules of Iran, there are some cases that are dedicated to computer and communicative devices. In article 4 of cyberspace states that "anyone who wants to have access to secret data and breaks the law of security measures of computer systems will be sentenced to between 6 and 24 months in prison or fine between 1o to 40 million or both of them at the same time. Article 9 also states that everyone transferring, spreading, deleting, sabotaging in computer or communicative devices or electromagnetic or light waves impermissibly will be sentenced to between 6 months and two years in prison or fine between 10 million to 40 million or both of them at the same time. Article 10 states that everyone blocking their access to data or computer or communicative devices by means of hiding data, changing the password or coding data impermissibly will be sentenced to between 91 days to one year or fine of between 5 and 20 million rial or both of them at the same time. Article 11 states that anyone do these aforementioned behavior for the purpose of endangering security, peace or public safety in articles 8, 9 and 10 and use these against computer and communicative devices that provides necessary and public services such as health service, water, electricity, gas, communication, transportation and banking will be punished to life in prison for between 3 and 10 years. (Fazli, 1388, 143)

5.6. Cyber-based stealing

Cyber-spaced stealing in article 12 of crime space has not been predicted. This kind of crime is cyberspace because stealing data as if it has not been stolen is like espionage and tapping that happens against secrecy of data. Therefore, it is classified as a crime in which computer is target it should not be mistaken with crime in which computer plays a key role on committing the crime. Cyber-based stealing is act of stealing someone else's property or of intruding without permission and satisfaction. The subject of cyber stealing is data. This data, according to article 12 of cyberspace crime, must belong to someone else whether this data is valuable like a formula or without any value like accepted article or the owner of data has created the data like the text of a book or the data has been bought from someone else or has been achieved legally.

Data that belongs to someone else must be placed in his computer or in a place where it is considered to be the legal place for that man. Therefore, if someone upload someone else's writing without any limitation, he is not considered to be robber but if someone steals someone else's essay even though the text is free on the internet, this action is prosecutable and punishable. Some of the laws and rules in Iran have been devoted to these kinds of crimes. Article 12- anyone who impermissibly steal someone else's data, if this data belongs to the owner, he will be sentenced to pay fine between 1 and 20 million rial unless he will be sentenced to between 91 and 1 year in prison or to fine between 5 and 20 million or both if them at the same time. Article 13- anyone using computer or communicative systems to do the actions such as entering, changing, deleting, stopping, intruding the system or phishing some amount of money, he will be sentenced to pay fine between 20 and 100 million or to spend period of 1 to 5 years in prison or both of them as well as paying the amount of money that he has stolen. (Jalal Farahani, 1383, 12)

5.7. Cyber Fraud

Cyber fraud is one of the crimes against properties and ownership and some of them are known as the crises of twentieth century. Cyber fraud like traditional crime is conducive to criminal result and sometimes it can be committed against property or asset in forms such as deletion, stopping or intrusion in computer system by means of misusing computer. In criminal law of cyberspace like traditional one, misusing computer software in order to get some money or benefits is the difference between cyberspace crime and other forms of crime (Najafi Abrand Abadi, Law journal, 1371). Cyber fraud is one of the crimes of so called "white collars" that has been developed by means of internet and communication. Fraud on the internet implies any kind of fraud that can be carried out by means of computer software and communication in internet network. For example, sites (web), electronic post (email) or chatrooms can be the means for cyber fraud in any forms in which some parts of the internet can be used for the purpose of defrauding. Therefore, it can be clear that cyber fraud become widesoread when internet was created and nearly "this crime has existed for two decades. Cyber fraud is stealing others' asset by means of using fraudulent operations malicious intention (Mir Mohammad Sadeghi, 1386). Article 12 and 13 of cyberspace crime that are mentioned above are the basics of this sort of crime.

5.8. Crimes against public security

Although these kinds of crimes breaching the security but on some occasions this feature is very crystal clear. On other words, this sort of crimes is in direct tie to notions such as national security and public safety.

5.8.1. Cyber Terrorism

As it can be seen in the title, it is made up of a series of actions that some particular people commits it with particular purpose and it can do a lot of financial and physical damages or casualties and for this reason it has been classifies as the most horrific crimes. The target of cyber terrorism is the computer systems and communication used for public services. This behavior is intentional and its final aim is put public safety and security at risk. On the other hand that criminal commits his crime by means of necessary public service system. In Iran, article 11 of cyberspace crimes has predicted this kind of crime without naming it as terrorism that is, in fact, very close to cyber terrorism and this called computer intrusion carried ou on purpose. Article 11- anyone committing the abovementioned deeds in articles 8, 9 and 10 on the purpose of jeopardizing the public safety and security and committing against computer and communicative systems used for doing services to the public such as health, water, electricity, communication services or transportation or banking will be sentenced to between 3 and 10 years in prison (Fazli, 1388, 125)

5.8.2. Cyber espionage

Cyber espionage means that someone gets valuable information by any means such as infiltration, tapping to damage the victim (Langroudi, Law terminology, 189, 1385). Article 3 of cyberspace crime- anyone commits the following crimes impermissibly in relation to secret data that is transferring or saving in computer or communicative systems: a. access to data or getting data or tapping transferring data will be sentenced to period of 1 and 3 years in prison or fine between 20 million and 60 million or both of them as the same time. B. make the data accessible for those who are not eligible to sentence between two and 10 years c. disclosure or make data accessible government, organization, company or alien group to sentence between 5 to 10 years. Note 1- secret data is sort of data that its disclosure will damage the national benefits or security. Note 2 the rulebook of determining secret data and its classification and protection will be passed within 3 month by collaboration between Information ministry, justice, interior, communication and military. According to article 4- anyone violate the security measures of computer and communicative systems with the purpose of having access to this data will be sentenced to the period of 6 and 24 months in prison or fine between 10 and 40 million or both of them at the same time. According to article 5- if office worker in charge of protecting this secret data of article 3 of this law or related systems create the opportunity for other eligible people to have access to this data owing to irresponsibility or imprudence, he will be sentenced to the period of 91 to 24 months in prison or fine between 5 and 40 million or both of them at the same time as well as suspense from work for 6 months (cyberspace crime).

5.8.3. Cyber forgery

Forgery literally has the meaning of distorting, changing, creating, making or placing (Moeen, 1375, 1230). Forgery is the act of creating or making fake document for the purpose that the forger or someone using this forged document coax someone else to accept this as the genuine one and consequently the victim has harmed himself. The crime of forgery is one of the crimes that put the public safety in danger and because makes documents worthless and create negative impression about documents, it must be punished severely. Cyber forgery is like traditional form of it on many occasions and there is only slight difference between them. Therefore, necessity of criminalization can be felt regarding the lack of authority of article 523 in Islamic punishment law. According to definition of document in civil law, it is defined as the writing that can be used as a piece of document and the writing must be real and tangible. Because this definition does not include the electronic documents, this article 523 cannot cover cyber fraud. In other words, the target of cyber fraud is data and information in the computer that is not similar to documents written by hand and it is legible only in the computer. Professor Suzan has stated in this respect that: the notion of forgery is the act of distorting documents in order to cheat. In the past, this distortion and manipulation had been carried out in paper documents. Nowadays, this happens both in paper and electronic ones." (Khodagholi, 1382) according to article 6 of cyberspace crime "anyone committing these following crimes impermissibly must be counted forger and he will be sentenced to period of 1 to 5 year in prison or fine between 20 and 100 million or both of them at the same time A: changing or creating documents that can be used as real one or distorting the real ones b. changing data or signs in memory cards or that can be processed in cards in computer and communicative systems or creating fraudulent data. In addition, according to article 7 of aforementioned la, anyone who uses this kind of data or cards chips will be sentenced to the above punishments if he knows that they are fake. Article 524, anyone who misuses the signature of supreme leader or any of the heads of three powers or gorged them intentionally will be sentenced to 3 to 15 years in prison (Islamic Punishment Law).

6. VIOLATION OF PRIVACY

Privacy means that one person or group can separate his or their data and therefore can disclose his information. The boundaries of privacy are different in various cultures and individuals but the main theme is similar. Privacy sometimes is related to being unknown i.e. inclination to be anonymous or being far from the public. The various kinds of privacies like economic or medical services or privacies on the internet and privacies of information. Degree of privacy of information is based on how the public receives it and it itself is dependent on time and space conditions. The notion of privacy is can influence security. For example misuse of information security in privacies can mean the right to the body. Nearly all countries have rules limiting privacy in some ways. For example law related to tax needs some information about profits or salary of a person. Sometimes the personal privacy is in contrast to freedom laws. Sometimes some laws can disclose public information that is considered to be privacy in some countries. Privacy is relative concept from the cultural perspective. I.e. it depends on the society culture and this is itself is dependent on economic conditions. Sometimes, personal information can be revealed on their own accord for example to gain some advantages, to promote at the time of participating in competition s and lotteries and so on. Disclosure of personal information can sometimes lead to misuse from others and identity theft (Fazli, 1388, 155).

6.1. Violation of informational privacy by citizens

In some cases that is allowable or not and it violates the privacy of information of citizens and the criminal is one of the citizens, it must be said that the first rule is that this action is allowable unless law has forbidden it explicitly because although the element of violation of privacy is not stated but the first rule is the liberty of their action. Therefore, there is doubt as to whether some examples are the violation of some rules. (Parvizi, 1382, 11)

6.2. The violation of privacy of information by government

In cases that an action has violated the privacy of citizens by government and government can violate based on some rules then the situation is complicated; because on the one hand it is stated that the first rule is the freedom of action and this is the same for all the criminal and because the basis of this rule is wisdom and regarding the fact that this is also applicable to the government, consequently there is no doubt that the action is allowable unless lawmaker has forbidden it. Therefore, lawmaker in article 558 of trading law and in entry 15 of law relating to legal personality states that " the legal personality should have all obligation and rights of ordinary people unless there are some rights and obligations that human naturally has it like parental duties and so on." Although the aforementioned article has illustrated the authorities of legal personality, but it must be kept in mind that the same law is the effect of article and in case the lawmaker has not made such a law, the legal personalities will be deprived of rights and obligations. In short, in some cases that law has allowed it, it is not conducive to the informational security by citizens and if the same action has been carried out by government, it is not allowable and the first law is that it is forbidden unless law has allowed it explicitly (Aslnai, 1389)

7. CONCLUSION

Knowing is one of the needs of human and the cyberspace has met this need very well and the users of this internet cyberspace are seeking to find out answers for the question they can not answer in the real world. IT has changed or rocked all the basics and foundations of the human lives such as discipline, security and the public safety at the incredible pace. Privacy is so vital that resprct to this domain has exceed the boundaries in religion and ethics and has found some legal guarantee but humanistic aspect and its protection has encountered some challenges and ethical health and even physical health of children and teens are at risk. In the meanwhile,

internet is suitable tool and medium to disseminate the thoughts and ideas everywhere on the condition that it must be used in the right way. People should have enough information in order not to have social and financial problems. Criminal protection is one of the dimensions of criminalization and it can be justified by means of criminalization and valuable basics. Using punishments for protect the values is the last step. If necessary, in issuing and execution, it must be paid attention to basics of criminal protection in order to get pleasant result by using it. It seems that security and privacy of people has been ignored more than ever and the rights of people have paled into significance. Regarding the importance of privacy and its effect on single individuals, we should find a solution to this dire problem. Although the problem of privacy is very fragile and subtle issue to borrow the phrase from Arthur Miller and there are dire problems in this domain. With all this in mind, to protect the privacy of people, actions such as legal solution, lawmaking, common law, sponsoring projects in respect to new techniques of coding. The encouragement of citizens to take part in process of making decisions either in national boundaries or international ones can be very effective in protecting this privacy.

REFRENCES

[1] Quran
[2] The universal decallration of human rights in1948
[3] Asani, laws of IT, Mizan pulication, 1st ed, 1384, p 100 onwards
[4] Ansari, Bagher (1383) the privacy and its protection is Islam Ruls, comparison and Iran, Jouranl of Law and Plitics of Tehran University, 1366.
[5] Ansari, Massod and Mohammadali Taheri (1386), private law thesi, vol 2, 2nd ed, Mehrab Ferk Publication, Tehran
[6] Boulek, Bernar; Criminalization. Trans: Ali Hossein Najafi, Tehran Majd Publication, 1382
[7] Parvizi, Reza, computer guilts pamphlets, center of studying judicial development, 1382
[8] Jafari langeroudi, Mohammad Jafar(1378), Expanded in law terminology, vol 3, 1 edit, Ganj Danesh publication, Tehran
[9] Jafari, Abbas(1385), analysis of privacy(first section), Ta'alee journal, issue1.
[10] Jalali Frahani, amir Hossein, prevention of cyberpace crimes, legislative journal, issue 1383
[11] Khodagholi, Zahra (1382), computer crimes, Aryan Publication, Tehran
[12] Fazli, Mehdi (1388), criminal responsibility in cyberspace, Thran, Khorsandi Publication Islamic Law Punishment passed in 1376
[13] Laws of cyberspace crimes passed in 1388
[14] Moeen, Mohammad, Persian dictionary, Tehran, Michael Publication, 1384
[15] Civil and political law convention passed in 1976
[16] Mir Mohammad Sadeghi, hossein (1386) Crimes against public safety and security, Mizan publication, 9th ed.
[17] Mir Mohammad Sadeghi, hossein (1386) Crimes against properties and ownership, Mizan publication, 19th ed.
[18] Nourabha, Reza, Laws of common punishment, Tehran, Dadafarin Publication, 1378.
[19] Article 13 of universal declaration of human rights, "everyone has the right to live, to have liberty and to have personal security."
[20] Article 12 of universal declaration of human rights, "no one should be disturbed in his private life or correspondence and his honor, name or reputation should never be invaded. Everyone has the right of protection against such invasions."
[21] Islamic Republic of Iran has joined after passing it in Islamic republic representatives in 1351/8/23

[22] Article 17 of international convention of civil and political in 1966: 1. No one should be disturbed in his private life or correspondence arbitrarily. 2. Everyone has the right of protection against such invasions."

[23] Article 16 of convention, 1. In private life, family, or personal correspondence, no child must be disturbed arbitrarily or illegally. 2. Each child has the right of protection against intrusion and violations.