PalArch's Journal of Archaeology of Egypt / Egyptology

CIVIL LIABILITY REGULATIONS FOR PRIVACY IN CYBERSPACE IN LINE WITH INFORMATION SECURITY

Homayoun Alihosseini[1], Hamidreza Alikarami[2], Rasool Ahmadifar[3]*
[1] Ph.D. Student of Private Law, Islamic Azad University, Arak Branch, Arak, Iran.
[2] Assistant Professor and Faculty Member at Islamic Azad University, Arak Branch, Arak, Iran.
[3] Assistant Professor and Faculty Member at Malayer University, Malayer, Iran.

*Email: alihosseini@cra.ir

Homayoun Alihosseini, Hamidreza Alikarami, Rasool Ahmadifar: Civil Liability Regulations for Privacy in Cyberspace in Line with Information Security -- Palarch's Journal Of Archaeology Of Egypt/Egyptology 18(4). ISSN 1567-214x

Keywords: Privacy, Cyberspace, Electronic intermediaries, Eavesdropping

ABSTRACT

Privacy is one of the basic concepts related to human rights, individual freedom, and human dignity; it has been taken into consideration in different legal and moral systems including Islamic and Iranian law. Privacy is an adaptive term in terms of terminology although, in terms of concepts and examples, it contains wide angles and rules in Islamic law. Common examples of considering privacy in Islamic law and Sharia are the prohibition of inspection, search, suspicion, eavesdropping, breach of trust, backbiting, insulting, and unauthorized entry. There are various rules regarding privacy in the Iranian Constitution, the Code of Criminal Procedure, the approvals of the Supreme Council of Cyberspace, the Islamic Penal Code, etc. Protecting privacy in cyberspace is a common and new example of privacy. Due to its technical conditions, cyberspace is of considerable capacity for misuse and violation of privacy. On one hand, common cases of the violation of privacy in the virtual environment are of considerable characteristics and, on the other hand, the emergence of the virtual environment has caused new areas of the violation of privacy. Based on the technical and legal characteristics of the virtual environment and activities, it is necessary to deal with the violation of privacy in these areas. Then, the significance, role, and execution of privacy protection in virtual environment need to be guaranteed. Subsequently, in order to effectively protect privacy in cyberspace, relevant laws have to be enacted by the legislature branch in cooperation with the executive branch to eliminate the serious gap.

INTRODUCTION

The concept of privacy, on one hand, is a result of human relationship and, on the other hand, the resistance against power-centered behaviors of the governments. From one perspective, privacy means a review of and reduction in the government's influence on people's life and relationship and, from another perspective, means humanitarian ideals; in sum, it is human rights. Privacy can be classified into five distinct but

related categories: physical privacy, spiritual privacy, information privacy, communication privacy, and privacy of places and things.

Although some legal concepts and rules like ownership have a long history, privacy and the related rules are new. There are various definitions of privacy in law and social norms. Privacy is a right that all humans in any country need to know because this awareness leads to the realization of citizenship rights. However, governments play a great role in this regard. Governments and legal systems have to update rules related to the privacy of citizens. Avoiding listening to telephone conversations, securing cyberspace, searching or locking personal files and data and so on are examples of the privacy of citizens. The legislator is in charge of developing a special legal system for them.

However, people's privacy is not violated only by governmental organizations. People may violate each other's privacy. When the privacy of a citizen is invaded by another citizen, they can refer to the government and judiciary power which practice law and social order; in this way, the invader is punished. This may not happen simply when the invader is the government. One can never punish the government for violating privacy. In its most favorable sense, the government can be obliged to compensate for the violation if the restrictions allow and conditions are provided. Anyway, in many cases, the actions of the government are seemingly lawful and deterrent.

Information and communication privacy in cyberspace is more at risk because of the likelihood of tracking and publishing the users' personal information. Therefore, it is necessary to stipulate serious rules for supporting this right in legal systems. The laws of different countries in this regard indicate different views toward this category; in Iran, based on the governmental structure as well as Islamic viewpoint toward this category, some frameworks have been specified. In other words, some measures are embedded within the laws of any country to protect personal privacy in cyberspace against the actions of individuals and government. In this regard, there are some rules in the Iranian legal system, which are explored in the present research.

Now, after the statement of the above problem, the following questions may arise.

1. What are the examples of privacy violation in cyberspace?
2. What are the main rules of Islamic jurisprudence concerning protecting privacy in cyberspace?
3. What issues are not taken into consideration by the legislator in stipulating supportive rules for privacy?
4. What is the basis of civil liability in cyberspace?

The significance of such research is related to the most basic subject in criminal law, i.e. the justification of the government power against free and independent people, a subject which is somehow a political and ethical philosophy. Sometimes, considering the public and private rights and freedoms that form them interfere with other values like security that demonstrate government authority followed by criminal law. This means that attempting to observe the interests related to public and private sector sometimes interfere with other values. For example, absolute defense of

privacy may damage the free flow of information which is necessary for the public sector, not for the government.

1. Definition of privacy, kinds and threats

1.1. Definition of privacy:

Generally, "privacy" is a flowing concept including various meanings such as freedom of thought, control over your body, control over your information, freedom from others' supervision, solitude and loneliness, protecting personality and credibility, and protecting against inspection and search.

Because of difficulty in defining privacy and determining its natural and formal framework, some theorists have not regarded an independent identity for privacy and they say one should refer to other fixed rules for protecting privacy. Therefore, there are two different approaches toward the independent identity of privacy at the present:

- Some have studied privacy with skeptical and critical views. They claim that there is no right to privacy; privacy is not new and does not indicate anything special.
- On the contrary, many theorists believe that privacy is a valuable and meaningful concept by itself.

Generally, these definitions are divided into six categories:

1. Privacy means having the right to loneliness.
2. Privacy means limited access of others to oneself and the capability to block unwanted access to individuals.
3. Privacy means confidentiality, i.e. hiding some affairs from others.
4. Privacy means having control over personal information.
5. Privacy means protecting personality and dignity.
6. Privacy means sincerity and intimacy.

Edward Bloustein considers the violation of privacy as an offensive action against human nobility, dignity, and integrity. He says: "The man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity. Such an individual merges with the mass. His opinions, being public, tend never to be different; his aspirations, being known, tend always to be conventionally accepted ones; his feelings, being openly exhibited, tend to lose their quality of unique personal warmth and to become the feelings of every man. Such a being, although sentient, is fungible; he is not an individual." (Ansari, 2004: 8).

Bloustein defines privacy as "The right of individuals to determine when, how, and to what extent to publicize their information" (Mohseni, 2010: 26).

In another perspective, privacy is considered a basic and important human right in Islam and includes:

1. The right of individuals for being alone in their private life
2. The right to protection against government supervision and interference

3. The right of not publicizing individuals' personal affairs without their permission
4. Protecting individuals and their place of life against search and record
5. Protecting information and thoughts against compulsory confession to a crime
6. Government's lack of right to oversee the individual private authority and the right to keep the information confidential (Berween, 2002: 72)

1.2. Types of privacy

1.2.1. Physical privacy (physical integrity of individuals)

The individuals who live in a country and are citizens of that country have the right to go wherever they want throughout the country, drive any vehicle they want, carry everything they like, and stop wherever they prefer providing that they do not exceed the legal framework and limits while enjoying this right. As the supporter and advocate of citizenship rights, the government needs to not only avoid violating this right but also prevent third parties from violating the right.

The physical integrity of individuals is the first and most obvious property of them and everyone is preferred to decide in this regard by themselves rather than others. Thus, any kind of inspection, body search, medical examinations and tests and the like as well as disclosure of the obtained information regarding these actions is only possible by receiving consent from the person; the violation of this unique right entails legal responsibility. Of course, like other forms of rights and privacy, this right is also absolute and without exception. In some cases such as legal order, cases related to public health, and discovering crimes against security, this right may be limited based on the contents of law.

The invasion of the physical integrity of individuals is the result of the said issue; however, it does not mean that there is no space for new discussion in this regard. On one hand, the issues and examples related to this right have been substantially developed because, in prior centuries, the information related to individuals' bodies and health had not been addressed as today. On the other hand, due to the development of information and communication technologies, the likelihood of abuse and spiritual and material losses caused by accessing, processing, and releasing such information has drastically increased.

1.2.2. Privacy at home

"The most important arena considered private before industrial developments and the emergence of modern technologies was individuals' place of living. Now, privacy at home is one of the most important categories of privacy.

Among all properties, domicile is of great significance since human uses home as a place for comfort and welfare and it is the most secluded place that can be imagined ever. Therefore, it is of special importance in society and everyone usually respects owning a home even if it is not mentioned in the law. In this regard, the kind and quality of domicile are not effective, what is important is that the place can be called a home" (Ansari, 2004: 28).

1.2.3. Privacy of communication (correspondence, letters, telecommunications)

Privacy of communication is used for dimensions of confidentiality and personhood of individuals' communication in society. Based on the rules governing this kind of privacy, everyone can expect to keep some of his individual and social communications unknown such that it is kept from public awareness and unauthorized individuals have no right to search, monitor, and intercept concerning them. This kind of privacy includes all human communications such as ordinary mail, email, and conversations through telephone, telegraph, internet, etc.

"Prohibited unauthorized listening to conversations, intercepting messages, opening letters, and disclosure of their contents are related to this kind of communication.

The basis of protection from and responsibility for the violation of privacy in communication, more than anything else, is related to the rule of respect for privacy and confidentiality from the perspectives of social norms and law. It is the most comprehensive basis which covers both material and spiritual aspects of privacy" (Ansari, 2004: 28).

1.2.4. Privacy in cyberspace

"Publicizing privacy and privatizing publication are discussed when deciding for globalization. In virtual life, "Publicizing privacy" and "privatizing publication" is not unlikely, too. Having ended media exclusiveness, the internet has provided individuals with bilateral interaction for developing thoughts. It is not possible to draw a border between private and public areas of the internet because of the growing changes. Although the global information and communication network has greatly developed the interaction between human beings, it has caused the violation of rights to a large extent" (Motamednejad, 2007: 75).

In this regard, the personal and confidential information which may be subjected to disclosure through the internet include all trademarks, private relations, religious or political affairs, medical information, and financial or security information. These pieces of information are saved on computer networks for different reasons such as easy access or transferring to other centers; they can be easily accessed by profiteers who disclose them and cause huge losses to the interests of individuals (Aqababaei, 2010: 58).

The privacy of individuals in cyberspace can be explored in two areas:

1. Private or nonpublic communications held simultaneously or asynchronously around the globe in different written, audial, visual, and even multimedia forms.
2. Databases containing personal information or even storing sensitive personal information of individuals and are not so difficult to access. Thus, it can be generally said that the privacy of individuals in cyberspace is invaded by criminals through four operations including production, collection, processing, and transferring data; in this way, criminals threaten the privacy of individuals (Ansari, 2008: 57).

However, the scope of virtual privacy has not been yet internationally agreed upon by the governments because achieving an

agreed single concept restricts governments from the implementation of their plans. To get rid of restrictions and not being bound to legal frameworks which might also be reflected in common law and constitution of the countries, some governments never agree upon the scope of formal and legal definitions so that they can violate privacy when needed.

1.3. Threats

1.3.1. Threats due to governments' authorization and inclination to control the private life of citizens

In every society, the government is the manifestation of public interest. Although it has ethical, religious, and economic aspects, it is not basically ethical, religious, and economic; it is of different functions including observing discipline and security, protecting fundamental rights of individuals, etc. The obligatory aspect has been emphasized in some theories of government. Enjoying the authority aspect which is a sustainable characteristic, the government has always imposed obligatory actions and behaviors. Hence, another important principle that assumes the identification of "the right to privacy" as an essential issue is the existence of the government with its power and domination in society. "On one hand, according to internal commitments to their citizens and with regard to international human rights requirements, any government is obliged to provide the conditions for the realization of the citizens' fundamental rights. On the other hand, the government may resort to the most severe tools or force majeure for its survival and polity. There will be no freedom and privacy if extreme security dominates society. However, security mechanisms are needed to be applied to guarantee these two categories. Therefore, some questions arise: How is it possible to strike a balance between the two? How long can a society survive in the name of security? And to what extent is it possible to sacrifice freedom at the expense of security? Maintaining national security and protecting privacy are essential rights for the survival of the citizens in a democratic society".

1.3.2. Inspection and body search

As mentioned earlier, the right to physical privacy may be violated in some cases by law enforcement agents, especially the disciplinary forces. An obvious example of this violation is the right of inspection and body search.

If it is not lawful, body search -more related to arrested people and common criminals- is one of the cases through which the individuals' freedom and personal security are violated because body search is an example of physical privacy violation. The violation of physical privacy becomes clearer when people are subjected to body search by police or other security forces with the excuse of preventing crimes. A clear example of body search is that which is performed on intercity travels by checkpoint inspectors without judicial writs or the body search performed before entering some offices which are not at a high level regarding security" (Ahmadi, 1998: 20).

1.3.3. Property inspection

Although security, health, and social needs entail inspecting public and even sometimes private places, the inspections should not exceed legal frameworks and violate individuals' privacy and public freedoms. Hence, this kind of privacy and its exceptional cases have been explicitly included in the legal systems of most of the countries.

In this regard, in the legal system of Iran, both personal and material privacy have been taken into account in Article 22 of the Iranian Constitution in which rights are regarded as an example of spiritual privacy and home is considered as material privacy. Regarding home, the concept and lexical meaning of home denote a place of residence that is often used simply for living; however, there are places which are used for a purpose other than a residence. Privacy of these places can be included in Article 22.

There are cases in which this kind of privacy is violated by laws that are contrary to this Article in practice or by law enforcement agents, for instance, disciplinary forces; they perform vehicle inspection in checkpoints and this is a common practice despite its legal prohibition.

A natural person complained about circular no. 402/01/179/1 dated 2000-07-01, that the general department of laws and legal affairs of NAJA has regarded vehicle inspection as lawful in case of non-flagrant crimes without obtaining permission from a judicial authority. They had even ignored the order of judicial authority regarding avoidance of illegal inspection. The Board of the Administrative Court of Justice, on 2001-08-19, with a lawsuit no. 177, regarded the job as contrary to the explicit content of Article 24 of the Code of Criminal Procedure and voted to annul this circular.

1.3.4. Invasion of information privacy

Article 7 of the Code of Statistical Center of Iran (1974) contains considerable points regarding data privacy. This Article states "Anyone who lives in Iran or Iranian citizens living abroad are obliged to correctly answer all censuses done by statistical centers of Iran. The information and statistics collected through different censuses from individuals and institutes will be kept confidential and shall not be used but for the preparation of general statistics. It will be never lawful to use, demand, and refer to the information collected from individuals and institutes in judicial, administrative, and tax affairs."

"Protecting privacy especially with regard to information and secrets is one of the most important individual rights because it is related to their dignity and personality. However, freedom of information and the right of society to know various news and information entails being informed of people's life. Therefore, these two rights are sometimes contradictory. On one hand, everyone has the right to the confidentiality of secrets in a way that others "should not know" about them and, on the other hand, society has the right to awareness, i.e. they need to "know". People have the right to know any news or information about individuals in society whether they are ordinary individuals or political and artistic figures. However, this right may be contradictory to the right to privacy, protection, and freedom in personal life. In many cases, others' awareness of personal secrets deprives one of comfort and security" (Faqih, 2010: 15).

In any country, the right to privacy should be inevitably in line with the interests of the government. For instance, access to medical information of people for engineering medical services and the promotion of the quality of life is always needed for policymakers. Many people in the world know that the government collects their personal information; they recognize the government's right to scrutiny and monitoring, too. The important point is that these rules are so weak and are not protected by sanctions. Besides, they are very defective and they have not prohibited the government from scrutiny and collecting individual information.

1.3.5. Threats due to modern technologies such as computer or monitoring devices

The most important factors challenging individuals' information privacy today briefly include:

1. Internet
2. Developing data storage and processing capacity of personal computers
3. Continuous and extensive monitoring of citizens in public (e.g., the police-monitored closed-circuit television cameras) and private places.
4. Geographical monitoring of the users of mobile telecommunications (like cell phones)
5. Drastic progress of technologies related to identification and personality traits (detecting information from DNA, retina, voice, a strand of hair, tooth, etc.)

Cases of the violation of privacy through modern technologies are provided below:

1. Identity theft via the internet
2. Interception and seizure of emails and internet communications
3. The use of microelectronic chips
4. Eavesdropping and intercepting telephone conversations
5. Violation of security measures of computer devices
6. Interference or destruction of data with computer or telecommunication devices
7. Disabling a database and prohibiting individuals from personal websites
8. Defamation through releasing voices and videos as well as roorback using computer devices

"Due to the emergence of modern information communication technologies, privacy in life has been endangered today. On one hand, the internet facilitates access, distortion and destruction of personal data in that individuals' identity may be subjected to illegal purposes. On the other hand, it provides the likelihood of tracking personal information and the contents of the messages. Any kind of personal information such as physical information, image, voice, sexual relationships, philosophical, religious, and political beliefs, racial and ethnic origins, and even the kind of interests and tastes shall be supported by the legislator as soon as they are processed through electronic data.

Moreover, since information technology has led to extensive sociopolitical developments, there have been new and unique ethical problems in this area that needs to be dealt with. In other words, individual privacy is now subjected to threats which did not exist before just like when nobody was at risk of electric shock before the emergence of electricity" (Rahmdel: 19).

In the 1960s, people in Europe were mostly concerned with the role of government in creating and using databases containing citizens' personal information. Although it was not a new matter, computer documents had enormously increased the tracking chance. Databases replaced bulky files and it was possible to reproduce a copy of them without needing any special space. As a result, the governments could use them more while it was not economical in the past. The governments were increasingly interested in storing more information about individuals so that they can retrieve them if needed. The stored information included fingerprints, addresses, relatives, jobs, social relations, political activities, and where the individuals had/had not traveled.

1.3.6. Threats due to criminal sabotage in cyberspace

The most important examples of violation of privacy in cyberspace include:

1. Unauthorized access to computer or telecommunication data such as hacking individuals' emails or accounts
2. Eavesdropping of contents being transmitted through computer or telecommunication devices such as using keyloggers and online-chat eavesdropping software, etc.
3. Unauthorized access to secret data being transmitted through computer, telecommunication, or data carrier devices or acquisition of and eavesdropping them
4. Making secret data being transmitted through computer, telecommunication, or data carrier devices available for unqualified people
5. Violating security measures of computer or telecommunication devices for accessing secret data being transmitted through computer, telecommunication, or data carrier devices
6. Illegal deletion, destruction, or disruption of data in computer, telecommunication, or data carrier systems
7. Disabling or disrupting computer or telecommunication systems illegally such as disabling web databases and prohibiting individuals from accessing their personal websites
8. Illegal Prohibition of authorized individuals from accessing computer or telecommunication data or systems
9. Theft of data belonging to others
10. Defamation through releasing the distorted voice or video of others by means of computer or telecommunication systems
11. Releasing roorback by means of computer or telecommunication systems in order to harm others or disturb public opinion

12. Selling or disclosing a password or any data or making them available which may cause unauthorized access to others' data, computer or telecommunication systems

2. Laws of Iran, Principles of Islamic jurisprudence

In the Iranian legal system, the important rules related to privacy in cyberspace entail criminal protection and include the Fourth Development Plan, Duties and Authorities of the Ministry of Information and Communications Technology (2003), Freedom of Information (2010-02-03), the Electronic Commerce Law of the Islamic Republic of Iran (2006-01-14), Act for Punishment of Persons Who Illegally Intervene in Audio and Visual Actions (2004-01-06), Computer Crimes Law (2009-05-26), Approvals of the Supreme Council of Cyberspace, the Communications Regulatory Commission and Regulations of Information Networks.

2.1. Constitution of the Islamic Republic of Iran

1. Article 22 of the Constitution states: "The dignity, life, property, rights, domicile, and occupations of people may not be violated unless sanctioned by law".

"Mentioning some points regarding this Article is necessary: 1. Occupation of people has been considered as protected from invasion. If job and work are assumed synonymous with each other, it is clear that many cases of workforce adjustment in factories and offices are examples of the invasion of privacy. 2. The term "rights" has various definitions and interpretations. The right to privacy can be regarded as one right of the individuals, too. 3. Individuals' dignity and life are regarded in this article; however, their body, i.e. the physical privacy has been ignored unless "life" connotes body" (Boroujerdi, 2006).

2. Article 23 of the Constitution points out: "Investigation into one's ideas is forbidden. No one can be subjected to questioning and aggression for merely holding an opinion".

3. Article 25 states: "It is forbidden to inspect letters and to confiscate them, to disclose telephone conversations, to disclose telegraphic and telex communications, to censor them and to stop their delivery. It is forbidden to wiretap conversations. All forms of inspection are forbidden except according to the law".

Regarding modern technologies, this article does not include all contents exchanged in cyberspace, emails, etc. Furthermore, "except according to the law" is regarded as authorized eavesdropping at the present, resulting in the violation of human privacy.

4. Article 39 states: "All forms of violation against the honor and dignity of any person who is legally arrested, detained, imprisoned, or sent into exile is prohibited and is subject to prosecution".

Do the governments have the right to access the former criminal records of a person who is detained by law and use those records which are considered private for him?

2.2. Special laws

Special laws are those which were stipulated in recent years in order to legalize the use of modern information and communication technology in

the country. In the Iranian legal system, the important rules related to privacy in cyberspace entail criminal protection and include:

- The Fourth Development Plan
- Duties and Authorities of the Ministry of Information and Communications Technology (2003)
- Freedom of Information (2010-02-03)
- The Electronic Commerce Law of the Islamic Republic of Iran (2006-01-14)
- Act for Punishment of Persons Who Illegally Intervene in Audio and Visual Actions (2004-01-06)
- Computer Crimes Law (2009-05-26)
- Approvals of the Supreme Council of Cyberspace
- The Sixth Development Plan
- The Charter of Citizenship Rights
- Regulations of Information Networks

The Islamic Penal Code also contains some articles related to information privacy which are provided below:

1. Article 641: Harassing phone calls or other telecommunication devices. “If an individual bothers someone by means of telephone or other telecommunication devices, in addition to the enforcement of the special laws of the telecommunication company, he will be subjected to imprisonment from 1 to 6 months”.
2. Article 648: Disclosure of secrets by all people who are confidant because of their occupation or profession: “If doctors, midwives and pharmacists, who are confidant because of their occupation or profession, disclose people secrets illegally, they will be condemned in prison from three months and one day to one year or pay cash punishment from 1,500,000 to 6,000,000 Rials”.
3. Article 582: The violation of communication privacy by an employee: “Any government employee or agent who opens, confiscates, destroys, inspects, records, eavesdrops, any postal parcel, telegraph, or telephone conversation, in cases other than provided by law, or divulges their content without the consent of their owners, shall be sentenced to 1 to 3 years imprisonment and the monetary fine of 6 to 18 million Rials”.
4. Articles 103 and 104 of the Code of Criminal Procedure for Public and Revolutionary Courts contain considerable rules about information privacy. Article 103 states: “Among the papers, documents, belongings, and other personal effects of the accused, only those related to the crime shall be secured and presented to the examining witness(es) if need be. The judge is bound to cautiously treat other documents and belongings, and he should not allow contents irrelevant to the crime to be revealed”.
5. Article 104 points out: “In cases where there is a need to inspect and detect mailing, telecom, audio and visual correspondences related to the accused, in connection with the investigation of a crime, the judge will inform the respective officers to confiscate [these materials] and send them to him or her. Once they are received, they will be presented to the accused, noted in the minutes, and attached to the file after being signed by the accused. Refusal of the accused to sign will be noted in

the minutes and in case the items are not of relative importance, and if the confiscation is not necessary, they will be returned to the owner obtaining an acknowledgment of receipt".

6. Article 31 of the Press Law (amended on 2000-04-18) states that: "Publication of articles that threaten to harm or disgrace a person or disclose his/her confidential affairs is prohibited and the guilty managing director shall be introduced to judiciary authorities and punished according to the Islamic penal code".

2.3. Principles of Islamic jurisprudence

The legal basis of the rules related to privacy in the Iranian legal system originates from principles, rules, and sources of Islamic jurisprudence. There are various verses, traditions (narrations), and hadiths regarding the necessity of respect to individuals' privacy. The dimensions of privacy that have been taken into account by Islamic verses and traditions include the prohibition of inspection, suspicion, blasphemy and insulting, backbiting, breach of trust, eavesdropping and voyeurism, unauthorized entry to homes, and spread of prostitution. It is not necessary to mention all the above dimensions in the present study and only the following holy verses are presented.

1. Verse 27 of Surah Al-Noor (about unauthorized entry to homes):

«یا ایهالذین آمنوا لاتدخلو بیوتاً غیر بیوتکم حتی تستانسوا و تسلموا علی اهلها»

(O believers! Do not enter any house other than your own until you have asked for permission and greeted its occupants.)

2. Verse 28 of Surah Al-Noor (about unauthorized entry to homes):

«فان لم تجدوا فیهآ احداً فلا تدخلوها حتی یؤذن لکم و ان قیل لکم ارجعوا فارجعوا هو ازکی لکم.»

(If you find no one at home, do not enter it until you have been given permission. And if you are asked to leave, then leave. That is purer for you.)

3. Verse 12 of Surah Al-Hujurat (about the prohibition of inspection, suspicion, and backbiting)

«یا ایها الذین آمنوا اجتنبوا کثیراً من الظّن اثم و لاتجسسوا و لا یغتب بعظکم بعضاً)»

(O believers! Avoid many suspicions, for indeed, some suspicions are sinful. And do not spy, nor backbite one another.)

2.4. The constituent elements

2.4.1. Material element

Methods of unauthorized access can be divided into technical (such as Trojan Horse and worms) and non-technical (methods based on social engineering knowledge, establishing a friendly relationship with the system administrator, impersonation, pretending that you are the authorized user, etc.) methods. These methods are explained below.

A Trojan horse or Trojan is a type of malware that is often disguised as a legitimate program that does not harm your computer. This superficially safe program carries malicious software and steals all your information easily. Of course, this program does anything if not opened. It is sent with an email, contains tempting messages, and in this way makes

the user open the mail. SubSeven is one of the most important Trojan horse programs. This kind of program can be presented as an exciting computer game. When the user receives it and starts gaming, the program steals his information. Worms are another kind of destructive programs aiming at defecting others' information. Leaving no trace, these programs transfer from one computer to another. Worms function like viruses; in other words, both of them use the hosts which are usually word or excel documents. Worms are also displaced when the documents are displaced.

IP: if you open a file with an exe suffix and do not know what it is, your IP is sent to the personal computer of the sender and, in this way, you have helped the hacker to a great extent. In fact, the hacker can access your personal computer and do whatever he wishes (deleting a file, stealing a file, sending a virus, etc.)[1].

The material element of unauthorized eavesdropping in Article 2 of the Computer Crimes Law is comprised of five components, all these components or the necessary and sufficient conditions should be provided.

First: the subject of the crime is the data which are being transmitted; it does not include static or stored data. The mention of "data being transmitted" is for separating the crime of unauthorized eavesdropping from other similar crimes. Therefore, if unauthorized eavesdropping is to gain access to data, or computer or telecommunication systems which are protected under security measures, the crime is not applied in Article 2 and is included in Article 1 (Amani: 19).

Second: the transmitting data must have eavesdropped through a non-public and confidential communication; otherwise, if the communication is public and free, the act will be deemed to be permitted. Non-public communications are those that are not allowed for the access and involvement of the public whereas public communications are those whose stipulation philosophy is to inform people and the public can access them. Third: the subject of the crime is "content"; to understand the meaning and concept, the legislator used content instead of data (Pakzad, 2009).

Fourth: in addition to systems, electromagnetic waves are means of crime which emphasizes carrying the contents through waves, nothing except these cases is subjected to Article 2. For example, if a person listens to the conversation between two persons near the door phone or simply eavesdrops the conversation between two persons, his act is not subjected to Article 2. Indeed, this article has attempted to include unauthorized eavesdropping of the common electronic communications in an extensive scope.

Fifth: the physical behavior of crime is eavesdropping which includes gaining information and indicates that, like unauthorized access, eavesdropping is an absolute crime and there is no need to take effect (Pakzad, 2009).

2.4.2. Mental element

Unauthorized access is regarded as an intentional crime. Without having any effect on the nature of the crime, the motive of unauthorized

[1] The methods of access to others' information and destructing them is available on: http://sakhi54.parsiblog.com/Posts/629

access is of different kinds. Criminal intent: because unauthorized access is considered as an absolute crime, is not bound to any result, and does not any specific intent, the general bad intent simply suffices for the realization of the mental element. The guilty must commit unauthorized access knowingly and deliberately. Criminal motive: this kind of motives include innocent (such as increasing system security, protecting systems against damages, developing technical and engineering knowledge, etc.) and sinister motives (such as grudge and revenge, fame-seeking, financial motives, jealousy, etc.). It is worthy to note that the aforementioned motives do not affect the nature of the crime. They may be regarded as mitigating factors at last (Taharri, 2005: 190).

According to the rules of Iran, unauthorized access is of some conditions. It is a crime usually committed by programmers and specialists in computer sciences. It has a completely technical nature and is regarded as an absolute computer crime because, firstly, is a crime related to computer systems and, secondly, it can be regarded as a crime against property only in the environment of cyber and computer systems regarding the traditional classification of crimes. Furthermore, it is an intentional, immediate, absolute, and non-flagrant crime.

The unauthorized eavesdropping of Article 2 in Computer Crimes Law needs a mental element just like any other crime and its mental element is bad intent, i.e. intentional intent. In the said article, “if a person eavesdrops a content, ….”, the verb “eavesdrop” does not refer to a person who unintentionally becomes aware of some news. The unauthorized eavesdropping of Article 2 in Computer Crimes Law needs a mental element just like any other crime. The individual must have the intention of doing any act which is forbidden by law; it is the same as the general bad intent. Thus, Article 2 is applicable only if the individual has committed the crime knowingly and deliberately. However, the presence of a particular bad intention in committing the said crime is not necessary. Although many crimes are committed for a particular purpose, for instance, harming others, the said crime is proved by achieving the general bad intent. Distinguishing the border between error and intention with regard to eavesdropping is important.

3. Principles of privacy in international documents

As a transnational and universal principle, protecting the privacy of individuals has been taken into consideration by international institutes and observing the privacy of individuals has been specified in many international documents. Therefore, there are general regulations embedded in important documents of human rights in order to protect the privacy of individuals; some of them constitute the basic pillar of protecting the privacy and some have directly dealt with protecting information and communication privacy.

3.1. Universal Declaration of Human Rights (December 10, 1948, United Nations General Assembly)

Article 12 of the Universal Declaration of Human Rights states: “No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation.

Everyone has the right to the protection of the law against such interference or attacks".

3.2. The Cairo Declaration on Human Rights in Islam (CDHRI) (the member states of the Organization of Islamic Cooperation)

Article 18 of the CDHRI points out: "(a) Everyone shall have the right to live in security for himself, his religion, his dependents, his honor and his property. (b) Everyone shall have the right to privacy in the conduct of his private affairs, in his home, among his family, with regard to his property and his relationships. It is not permitted to spy on him, to place him under surveillance or to besmirch his good name. The State shall protect him from arbitrary interference. (c) A private residence is inviolable in all cases. It will not be entered without permission from its inhabitants or in any unlawful manner, nor shall it be demolished or confiscated and its dwellers evicted".

3.3. International Covenant on Civil and Political Rights (1966)

Article 17: "1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honor and reputation. 2. Everyone has the right to the protection of the law against such interference or attacks".

(The Iranian government joined this treaty in 1975. According to Article 9 of the Civil Code of Iran, the treaties held between Iran and other governments regarding the Iranian Constitution are deemed as law.)

3.4. International Convention on the Elimination of All Forms of Racial Discrimination (1966)

According to article 5: "The right to security of person and protection by the State against violence or bodily harm, whether inflicted by government officials or by any individual group or institution".

Despite the existence of various international documents enshrining the right to privacy, a question may be posed whether this right has been only recognized in international treaties and documents and is of contractual authenticity or it can be claimed to become a social norm, too. In this regard, it is needed to be mentioned that although this right has been considered in a limited number of documents, if it is assumed as a category of human rights and the human right is regarded as an obligatory international norm, the right to privacy also receives customary reliability and is placed on the realm of international law.

3.5. The European Convention for the Protection of Human Rights and Fundamental Freedoms

The above convention has been adopted by the Council of Europe. It is a general obligatory treaty for the protection of human rights and fundamental freedoms which encompasses various rights and freedoms and it is obligatory for the member states to consider its contents in practice. It is regarded as a regional document because it is specified for a specific region.

Article 8 of the European Convention on Human Rights states: "1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".

3.6. Convention on Cybercrime (Budapest, 2001)

The convention consists of 48 articles and 4 chapters. The first section of chapter two is about substantive criminal law. The issues introduced in this convention provided a brief explanation of crimes related to privacy in cyberspace.

3.7. Approvals of the International Telecommunication Union (ITU)

ITU is an international organization affiliated with the United Nations. Based in Geneva, Switzerland, this union is responsible for legislation and administration of the radio frequency spectrum, the stipulation of standards for data and information exchange, and facilitating the growth and development of communications around the globe.

4. General Principles of the Liabilities of Electronic Intermediaries

Fault is a necessary element for the civil liability of electronic communication intermediaries. Fault or negligence in cases of violation is a duty which is imposed on the individual by law, contracts, or social norms. The concept of fault includes doing acts that should not be done and quitting acts that should be done (encroachment and negligence). As a result, to understand the fault of a person, it is needed first to identify the duties of that person in doing or quitting an act; then, violation of it is regarded as fault.

Fault is defined in the Civil Code of Iran. Article 953 states: "Fault includes excessive use and negligence". Article 951 also defines an element of fault, i.e. "negligence", as "Encroachment (ta'addi) consists of conduct surpassing the limits of permission or ordinary usage, in relation to a thing or a right belonging to another". Article 952 defines "negligence" as: "Negligence (tafrit) consists of omission of an act which, in virtue of an agreement of by ordinary usage, is necessary for the protection of another's property".

The liability of electronic intermediaries, like other individuals, is conditional upon the clarification of their fault. They are liable if it is proved that they have committed or quitted an act that a cautious person could not commit under the same conditions.

In the legal system of Iran, according to Article 1 of the Civil Liability Law, there is no hesitation regarding the acceptance of fault liability. Therefore, fault is the necessary element for the liability of intermediaries; the limits and the manner of recognizing fault depend on the intermediaries' type of activity and legal duties. Besides, the defectiveness

or weakness of computers in government and private institutes is regarded as fault in Article 78 of the Electronic Law of Iran. Hence, if it becomes transparent that damages have been caused due to the weakness of the computers of an access provider or the like regarding data security protection or their confidentiality, or the weakness of computers in preventing the release of unauthorized published works or violating others' copyright, the intermediary who was legally and logically supposed to provide appropriate computer facilities for preventing the said damages is deemed to be guilty and will be liable according to Article 78 of the Electronic Law and Article 1 of the Civil Liability Law. Moreover, regarding the regulations related to the activities of media, some liabilities have been defined for electronic intermediaries and violation of them is regarded as fault and entails liability.

Regarding the general principles of liability due to the violation of privacy in cyberspace, it can be mentioned that the theory of fault is accepted as a principle in the legal systems of the world at the present such that while discussing the liability of intermediaries, the necessary element of "fault" or "negligence" is taken into account. The liability of intermediaries is mentioned under the terms of "liability due to fault" and "negligence" in the existing legal doctrine, judicial decisions, and the published books and papers regarding the civil liability of electronic intermediaries in most of the countries. The reason for the application of the theory of fault with regard to the liability of intermediaries is related to the role of electronic intermediaries. Basically, the individuals who play an intermediary role in doing something lack absolute liability. In the Iranian legal system, individuals like business representatives, commission agents, brokers, lawyers, and forwarding agents (in the Civil Code) who become the intermediaries of doing an act, are known as a trustee and bear liability only in the cases fault. However, absolute liabilities may be deemed for them in cases where the professional liability of such individuals necessitates.

Fault-based liability has been approved as a basis regarding electronic intermediaries in different legal systems. As mentioned earlier, the reason for this approval is the legal role and position of intermediaries in causing losses. It means that a harmful act may be basically direct or indirect.

4.1. The activity of intermediaries as public data carriers

Electronic intermediaries in its specific sense, i.e. Internet service providers (ISPs) and hosted service providers are merely engaged in intermediary activities of transmitting and storing individuals' data; they have no control or inspection over the content of the exchanging information. Therefore, ISPs should not be legally subjected to liability for publishing and inserting offensive contents or false information and the like except for cases where they have been informed of the illegal contents or must be informed, or if they participate in publishing and inserting the information. In the latter sense, they may be regarded liable as a "publisher".

In fact, the "distributor" completes the last step of reporting activities and the process of producing works related to information and

communication technology to be used by the users. They provide the users with the works of others such as scientific, political, and religious papers, computer software, images, and the like.

Service providers may operate commercially such that they receive the needed license from telecommunication operators with a definite capacity based on their tentative users and provide the home internet users and commercial users with access to the internet by receiving money.

4.2. The duty of intermediaries with regard to content monitoring

Is a public data carrier institute responsible for controlling and monitoring data contents or not? This question is particularly posed for telecommunication operators in charge of transmitting calls and text messages. Are the mobile telecommunication companies of Iran which are in charge of transmitting all mobile text messages, or the operators such as Hamrahe Aval, Irancel, and RighTel in charge of monitoring SMS contents? From the perspectives of mobile telecommunication users, the service provider companies must not monitor the contents of their messages. Regarding the positive laws of different countries such as Iran, the USA, and the like, eavesdropping, wiretap, and intercepting electronic messages are forbidden. Article 25 of the Iranian Constitution remarks that it is forbidden to inspect, disclose, or wiretap telephone conversations or all forms of inspection except according to law. Article 528 of the Islamic Penal Code emphasizes this point, too.

Therefore, no responsibility has been defined for the related institutes and organizations like public data carrier institutes such as the telecommunication company, post office, ISPs, and other operators to monitor the contents of correspondences, conversations, and messages of the users; any inspection and monitoring in this regard is regarded as a criminal act except in cases permitted by law.

4.3. Lack of an obligation to monitor contents

Electronic intermediaries do not play the role of a publisher in the process of data processing and electronic exchanges and communications. They are either a public data carrier in cases where the information receiver is a specific person, or a distributor of information to individuals other than the sender. In both cases, the electronic intermediaries have not been allowed to monitor and control the electronic contents by the legal systems of different countries. Even in many cases such as the laws related to the protection of data or the electronic wired or wireless communications, the service provider units responsible for establishing connections have been forbidden from all forms of inspection, monitoring, and eavesdropping. In the Iranian legal system, Article 25 of the Constitution and Article 528 of the Islamic penal code clarify the prohibition of all forms of eavesdropping, unauthorized wiretap and monitoring of telephone conversations, correspondences and letters. Thus, generally speaking, it can be said that post and telecommunication intermediaries are not bound to inspect the contents of the clients' conversations, letters, and correspondences and are even forbidden from doing that. The positive laws do not include explicit orders regarding internet communications.

Article 5.3.1. of the regulations targeting ISPs which were approved by the Supreme Council of the Cultural Revolution states that: "ISPs and their subscribers are responsible for the content they distribute on the network".

Article 5.3.4. points out: "The responsibility of ISPs regarding the information distributed by others is limited to the implementation of network filtering".

Article 5.3.15. has also forbidden the ISPs from unauthorized access to subscribers' information privacy.

Hence, in the present legal system of Iran, according to the approval of the Supreme Council of the Cultural Revolution, Article 25 of the Iranian Constitution, and Article 528 of the Islamic Penal Code, the electronic intermediaries lack the qualification of content inspection and control. They are only bound to provide the Ministry of Information and Communications Technology of Iran with the general information of the users and the history of their internet activities; the ISPs are obliged to provide the facilities for network filtering (Article 5.3.3.) so that they can omit the information containing illegal contents, if necessary. Thus, the knowledge and awareness of an ISP regarding illegal contents is the necessary condition for electronic intermediaries. If an ISP or electronic intermediary such as telecommunication operators transmit data, conversations, and information containing illegal contents, they will be regarded liable if they know about the illegal contents.

In the Iranian legal system, too, the intermediary may be regarded liable for cooperating in the distribution of illegal contents. If an intermediary is aware of the offensive content and cooperates in distributing it via SMS or email, he will not be regarded as innocent.

There are various rules and regulations in Iranian law protecting all forms of privacy, especially privacy in cyberspace. They include respecting the legitimate freedoms and maintaining the civil rights (approved in 2004), Code of Criminal Procedure, the approvals of the Supreme Council of Cultural Revolution (comprised of three regulations: 1. The regulation for Access Service Provider (ASP) (approved in 2001). 2. The regulations targeting ISPs. 3. Guidelines for Internet cafes), the Electronic Commerce Law (approved on 2004-01-07), the approvals of the Supreme Council of Cyberspace, and the approvals of the Communications Regulatory Commission.

Regarding the punishment for privacy violation in cyberspace, it can be said that Articles 23, 19, 20, 22, and 40 of the Constitution of the Islamic Republic of Iran have forbidden any kind of violation of personality, life, property, rights, domicile, beliefs, occupation, and personal information of individuals. Moreover, privacy has been emphasized in Computer Crimes Law and Instances of Criminal Web Content in Cyberspace and different punishments have been considered for violation of this right. Article 1 of chapter 1of this law, titled crimes against the confidentiality of computer and telecommunication data and systems, states that every person who, without authority, gains access to data, or computer or telecommunication systems which are protected under security measures shall be punished by a term of 91 days to 1 year of imprisonment, or by a fine of 5,000,000 to 20,000,000 Rials, or by both the imprisonment and fine. According to

Articles 3, 12 and 10 and other articles of the Computer Crimes Law, wiretap or disclosure of information, data omission or destruction, data destruction and manipulation, hiding data and instances of criminal web content shall be subjected to specific and definite punishments.

CONCLUSION

Although the literature review demonstrates that privacy has been introduced in all societies to some extent, the concerns regarding the protection of privacy are serious in the present societies which are due to various developments of the recent century which are globally increasing. One of the most important developments is recognizing individual identity and related rights and freedoms. This kind of development has occurred simultaneously with scientific and technological developments; hence, it doubles the significance of maintaining privacy. Generally, there are two criteria for identifying instances of privacy:

1. Typical criterion: some aspects of human life are typically or conventionally regarded as private.
2. Personal criterion: some aspects of human life are not typically or conventionally regarded as private; people may consider them as a part of their personal matters and regard them in their scope of privacy.

Many countries have considered and approved special rules and regulations to protect privacy in physical space and private data in cyberspace. Therefore, in this regard, it is hoped that the Executive and Legislature branches of the Islamic Republic of Iran attempt to play a substantial role in stabilizing private and citizenship rights in cyberspace and physical space by preparing and developing a plan or bill for protecting privacy including the following components:

Personal information (body and soul), public and private places, domiciles, inspection, detection, the Hijab of men and women, place of occupation, ordinary and political prisoners, detention, etc.

REFERENCES

Aghababaei, H. (2010). The scope of security in Criminal Law. Tehran: Research Institute for Islamic Culture and Thought.

Ansari, B. (2004). Privacy and protection in the adaptive Islamic law of Iran. Journal of Law and Political Science, University of Tehran, 66.

Ansari, B. (2008). Freedom of information. Tehran: Dadgostar Publications.

Ansari, B. (2011). Mass communication rights. 4th ed., Tehran: SAMT Publications.

Berween, M. (2002). The Fundamental Human Rights: An Islamic perspective, The International Journal of Human rights, 6 (4).

Boroujerdi, M. (2006). Privacy in the information society. Hemayat Newspaper, 2 (15).

Faqih, A. (2010). Citizenship privacy, Fiqh and Communications Law. Baqir al-Olum University, 1.

Mohseni, F. (2010). Information privacy. Tehran: Imam Sadiq University.

Motamednejad, K. (2007). Communications Law. Tehran: Office of Media Studies and Development.

Pakzad, B. (2009). Cyberterrorism. Ph.D. dissertation, Tehran: Shahid Beheshti University.

Qanavati, J., & Javer, H. (2011). The basis of respect in identifying and protecting privacy. Tehran: Journal of Islamic Law, 8 (29).

Rahmdel, M. (2006). Human's right to privacy. Journal of Law and Political Science, University of Tehran.

http://sakhi54.parsiblog.com/Posts/629

http://www.maavanews.ir/tabid/38/ctl/Edit/mid/384/Code/6665/Default.aspx.