The holy Quran and tradition`s moral principles for prevention of cyber crimes

Mohammad Ali Ameri[1]
Jalal Ansari[2]
Mostafa Moradi[3]

Abstract

Cyberspace has become prevalent in the lives of millions people, but as much as it has turned into a tool of entertainment, gathering knowledge and information, it has deviated from the moral principles. Islamic ethics consists of moral guidelines which shows the right path to human beings including the manner of using the information technology based on the human morality. There are various examples of these principles in the Qur'an and Sunnah, such as fulfilling the covenant, enjoining the good and forbidding the evil, or other cases, which in addition to their functions in preventing sin, can also be effective in preventing cybercrime as well. This study is based on a descriptive and analytical method, and its findings show that the principles of Islamic ethics in the Qur'an and Sunnah are appropriate for all nations and times and when applied, lead to the creation of a moral society and subsequent success in crime prevention.

Keywords: Islamic ethics, cyber ethics, Quran and Sunnah, cybercrime, preventio

1. Assistant Professor and Faculty Member of NAJA Institute of Law Enforcement Sciences and Social Studies: M.ali.ameri.h@gmail.com
2. PhD student in criminal law and criminology and university lecturer, jalalansari@yahoo.com
3. Master of degree in criminal law and criminology: Moradi.m11985@yaho.com

Introduction:

Cyberspace or information technology have been pervasive in the lives of millions people around the world and become a tool needed by all human beings for fun, gathering knowledge and information, etc. and turned into a new dimension in our lives. For this reason, the penetration rate of the Internet is increasing in the society, and therefore, naturally, the statistics of crime, victimization and damage to moral issues in cyberspace are increasing day by day. New and mass media, which are mainly based on electronic communications and cyberspace, are developing every day, therefore, many criticisms are raised about the lack of attention to Islamic ethics in cyberspace and its practical role in prevention of crime; because obscene and blatant information and content and cybercrime, which were initially limited in scope, have become a matter of national and international concern with the development of the Internet (Hilliard, Keith, 2007, xi).

In most countries, especially in Islamic countries, everyone wants to use cyberspace in which moral principles are observed, but these principles can be different in each country and culture and in some ways have similarities; for example, production and distribution of pornography in Islamic countries are generally forbidden and immoral in real and virtual space, but in many Western countries this will not be immoral if it is in line with the law, and the issue of copyright and the age of the doers are observed. Cyberspace is frequently illegally used around the world against its moral principles. The previously recognized and enshrined rights of cyberspace are being violated daily in the name of economic progress, political stability, religious interests, the fight against terrorism, or for personal interests. The violation of these rights has created new

problems in the social systems that govern society, as well as advances in cyberspace that sometimes violate ethical principles and issues, such as cybercrime, digital security, and security concerns regarding the prevention of these crimes.

Although our information systems have evolved from data processing and information systems, to artificial intelligence and institutionalized systems, but there has not been considerable advances in the ethical issues of these technologies and their function in preventing and controlling cybercrime (Lester, 2016, 3). Agbourne's theory of cultural backwardness shows that technology has progressed faster than the ethical infrastructure needed to control and support these achievements (Marshall, 1999, 81-82). For this reason, ethics is essential for investigating and preventing crimes and abuses related to cyberspace.

For example, if people who are entrusted with the information of others , abuse such information they have violated that information, and this act is a widespread violation of trustworthiness as one of the moral principles in Islam. Therefore, recognizing and understanding immoral behavior in cyberspace can help to explain the strategies to deal with these immoralities. Of course, there are new examples of the effects of cyber-immoral behaviors, including problems with software theft, virus development, illegal access, and fraud. Such unacceptable behavior imposes great costs on individuals every year (Gilbert, Stead, 2001, 76). It is generally believed that the advancement of science and the pervasiveness of cyberspace have also damaged the ethics of this space. In other words, the lack of attention and not using Islamic moral principles in Muslim societies and even in the whole world in parallel with the development of cyberspace, have

led to less attention to such issues to control and prevent these crimes.

Therefore, it is vital to pay attention to the laws and principles of Islamic ethics and the principles governing them in order to expand legal-ethical research to help bridge the gap between behavior and advances in information science.

Given the above, the main purpose of the present study is to combine Islamic ethics with the ethics governing cyberspace, in the sense that we should combine the moral principles of Islam with the ethical principles governing cyberspace and present the ethical principles governing cyberspace, which are based on the moral principles of Islam, so that ,in addition to the theories of prevention-based criminology that have been accepted in most of the world, we can also use Islamic ethical principles in the field of control and prevention of cybercrime. In addition, this article intends to look at the following:

1. Investigating a number of the concepts and principles of Islamic ethics and ethics related to cyberspace
2. Developing some ethical principles related to cyberspace in the form of identifying examples and its functions for cyberspace users, especially Muslims from an Islamic and public perspective in order to control and prevent cybercrime
3. Identifying legal-ethical challenges and obstacles in the field of combining Islamic ethics with cyber ethics and providing suggestions for overcoming obstacles.

In addition to the above, it should be noted that technology is a double-edged sword. A student can use it for academic work or spend time on inappropriate sites (Ahn, 2006, 91). Trying to control people and prevent them from abusing cyberspace can easily be neutralized by bringing up the

issue of individual privacy. Also, cyberspace users can often be abused accidentally by other users, leading to privacy violation, fraud, theft, and even child abuse by child abusers. Rarely do those who publish their address and other identifiable information in cyberspace, think that they have provided valuable ways and means to be abused by a kidnapper or swindler. It has been said that new media can disrupt the social foundation of a society, so there are good reasons to study the ethics of cyberspace and the function of Islamic ethics in controlling and preventing these crimes, which are mentioned below:

1. Islam forbids all kinds of immoral and criminal activities in any area of human life.
2. The general public is not familiar with the Islamic moral principles governing cyberspace and their function in preventing and controlling crime, as well as the harms of not paying attention to these principles (Maghaireh, 2008, 337-338).
3. Familiarity with Islamic ethical principles makes every user behave responsibly in cyberspace.
4. We must study Islamic ethics and its principles that govern cyberspace because they can teach us how not to fall into the trap of criminals and that we ourselves adhere to these principles and do not commit crimes.
5. The ethics of cyberspace (which will be explained in the following) and familiarity and adherence to it to avoid illegal and immoral use of this space is vital for users, which requires some independent discussion of ethical issues.

Background:

The concept of information ethics which was developed in the 1980s, seeks to demonstrate the importance and function of values and traditions in cyberspace. This concept can be

different for each society in addition to commonalities because the ethical principles governing different societies are different. This concept seeks to establish "a standard for judging the behavior of an individual or a member of society, as well as for classifying these matters as moral and immoral" (Anna, 2006, 92). Information ethics is a relatively new branch of study that includes several distinct yet related subfields, including intellectual property, privacy, freedom of expression, and social control of information (Patterson, 2002, 346-347).

The ethics branch of information technology is currently not organized in a coherent way in most of the world, especially in Islamic countries, but in some countries, there are groups that have developed ethical guidelines. One of the most well-known and common is the ACM (American Computer Machinery Association), which provides ethical guidelines and professional conduct that were enacted in 1992. ACM Principles of Ethics is the most comprehensive guide to bridging the gap between cyberspace and ethics, the content of which will be briefly reviewed in sections to analyze how to adjust it to Islamic ethics.

With the explanations provided, it has been shown that guidelines based on ethical principles can be more effective on individuals (Sims, Brickman, 2003, 243-244). Therefore, the principles of Islamic ethics can be expanded in accordance with cyberspace by creating a culture (Couger, 1989, 212). Raphael Capuro reminded us that morality is a self-reference thing,that is, it is morality that paves the way for moral and human communication (Froehlich, 2000, 278; Lourdu, 2012, 1). Therefore, examining the nature of cyber ethics and understanding these issues can lead to better programs to strengthen moral education and improve the moral behavior accepted by Islam in cyberspace, and then

we can look for a combination of Islamic ethics and cyber ethics to so that we can teach and apply Islamic moral principles in order to prevent crimes and even prevent casualties in cyberspace.

The concept of Islamic ethics and ethics of cyberspace:

The word Akhlagh (morality), which comes from creation, literally means nature, (Qayyumi, 1418, 96) and technically refers to mental and spiritual characteristics that cause human actions to arise from the soul (Amini; Sharif Zadeh, 2015, 153). One of the foreign thinker believes that the best definition for ethics is as follows: ethics and moral principles are the best way to study the behavior of human beings and each of these principles must pursue a goal that determines the way we should behave (Iacovino, 2002, 57).

In another definition, ethics has been defined as a set of principles that distinguish what is wrong from what is right (Wood, 1385, 53-52). By accepting this definition, we can say that ethics is a domain for what is the norm in a society , because it states that one should do or avoid doing something. Ethical principles are the moral and spiritual standards that guide behavior, action, and choice. Ethics is based on the concepts of responsibility (as a free moral agent, stating that individuals are responsible for the actions they take) and accountability (individuals and society must be accountable for the consequences of their actions). In most societies, a legal system adopts the most important norms and ethical principles and provides a mechanism for doing so and pursuing individuals, and even accountable governments (Iacovino, 2002, 63-64) in the country. We can also find some of these principles that have been approved in the form of laws based on Islamic sources and Islamic

ethics, such as being trustworthy, enjoining the good and forbidding the evil.

Feiz Kashani defines ethics as a set of a strong rules which facilitate doing various things. If such items are based on the wisdom and law, they are called ethical and if the actions are frowned upon by the society they are called unethical. (Feiz Kashani, 1980, 5/95). Allama Tabatabayi states that ethics can be defined as virtues which are not gained voluntarily but can be acquired through learning the basics. He is one of the individuals believing that virtues and moral acts can be gained through repetition (Tabatabayi, al-Mizan, 1417,1/351).

In the definition of ethics governing cyberspace, it is stated that the ethics of cyberspace means the philosophical study of ethics related to computers and cyberspace and includes the study of behaviors that the user must adhere to. In this regard, the studying of the effect of adherence and non-adherence to these behaviors is also emphasized (Kanali, 2010, 1-3). Therefore, it is clear that in a world where social networks and cyberspace are defined by the way people live and work and strongly influence Islamic culture and values, it is important for us to investigate the principles of Islamic ethics, social responsibility which is a difficult task due to the diversity of beliefs, groups, classes, languages, dialects and cultures that exist in our country.

Typology of Islamic Ethical Principles (used in the Holy Quran and Sunnah):

Islam is the last religion that God Almighty sent to the people through the great prophet of Islam, Muhammad (PBUH). God has stated in the Holy Qur'an: "On this day I have completed your religion for you, I have completed My mercy on you, and I have chosen Islam as your religion" (al-

Ma'ida, 3). The Holy Quran contains more than 6000 verses; with hundreds of verses focusing on the moral aspects. The sources of Islamic law consist of the Qur'an, Sunnah, reason and consensus, here we focus on the Qur'an and Sunnah, because we try to understand the basic moral principles of Islam in these two sources and integrate them with the ethics of cyberspace and examine their function in preventing crimes in cyberspace. According to Shiite jurists, the deeds, words and speeches of the infallible Imams and the Prophet of Islam all form a tradition in Islam (Khorramshad, 1390, 117).

In any case, the general understanding of morality in Islam can be known as "a set of moral principles and guidance that distinguishes right behavior from what is wrong or what should or should not be done." The Qur'an and Sunnah show that all aspects of Muslim life should be guided by Islamic ethics. God says: "Surely this Qur'an leads you to that which is right (or stable)" (al-Isra ': 9). In the Holy Qur'an, God uses the term morality or character to refer to moral principles. The importance of morality in Islam can be seen in other Qur'anic verses. Also, the Prophet Muhammad (PBUH) said: "Indeed, I have been sent to perfect moral virtues" (Majlisi, 1403, vol. 68, 382). Therefore, according to the above, it can be said that the Qur'an can be the main source for extracting the principles of morality in Islam.

The moral system of Islam is different from the secular moral system as well as from the moral law advocated by other religions. Throughout the history of civilization, these secular models have been transient and inherited moral laws because they were based on the values of their human founders, for example, the Epicurean philosophy (philosophy of luxury) or the pleasure of attaining Happiness (Dehghanzadeh; Ahmadian, 2016, 145-146). In

contrast, the moral guidelines embedded in Islamic ethics emphasize the relationship between man and his Creator and consider religious ethics as the ethics of love or affection for God (Khazaei, 1387, 91). Because God is fully aware of everything, Muslims have instructions that are neither timed nor distorted by human whims and desires, hence the instructions of Islamic ethics can be applied at all times and in all places. The Qur'an and Sunnah use a set of moral terms to describe the concept of good, such as: truth , goodness, wisdom mercy, justice and fairness, balance and perfection, enjoining the good and forbidding the evil (known and confirmed), trustworthiness (honesty), sincerity (sincerity of intention) and piety (fear of God). Benevolent acts are described as righteous and illegal and infidel acts are described as evil. Some of these terms are repeated in dozens of verses of the Qur'an as well as in the Sunnah. This table shows the results (frequency based on verses and hadiths) for the moral principles and examples used in the Qur'an and the confirmed sources of the Sunnah.

Table 1: Frequency of the principles of Islamic ethics in the Qur'an and Sunnah[1]

Number of hadiths	Number of Quranic verses	Basics of Islamic ethics
66	65	Trustworthiness and honesty
145	595	Faith and piety
50	31	Fulfilling one's promises
142	235	Being grateful to God
124	227	Affection and kindness
34	23	Sincerity
29	66	Benevolence
100	202	Asking for forgiveness and

1. In relation to the frequency of hadiths in the field of Islamic ethics, It should be noted that the statistics in the table are the result of research by authors that have been collected by studying the authentic books of hadith.

		repentance
33	13	Enjoining the good and forbidding the evil
82	67	Guiding and correcting wrong behaviors
139	530	Knowledge and hard work
48	83	Contemplation
24	96	Human dignity
250	61	Being good tempered in relationships and business
62	23	Justice
64	108	Patience
31	129	wisdom
44	92	Honesty(truth)

This large number of verses and hadiths shows the support of the religion of Islam for people who observe good moral qualities, and on the other hand, warns, forbids or punishes those who do not observe these principles. Islam considers morality as an essential factor in the development or reconstruction of society based on the understanding of the Qur'an and Sunnah, which is a moral reconstruction in human behavior and can bring benefit, peace and prosperity to human beings.

According to the above, it is clear that the concept and application of these principles are close to the concept and application of various types of prevention, for example, faith and piety, enjoining the good and forbidding the evil, contemplation and patience, which are examples of Islamic ethics. In terms of function and sometimes concept, they have the ability to be adapted to situational prevention. Circumstances are related to the pre-crime situation of the person and lead the perpetrator to commit a criminal act (Pourshakibaei; Jahani, 2018, 38).

According to the previous explanations, this type of prevention and the mentioned ethical principles aim to prevent the occurrence of crime, by reducing the advantages of the crime and making individuals think about the actions before committing them .With the belief and commitment to these principles, a cyberspace user automatically refuses to do actions that violate these principles.

Another issue is the application of examples of Islamic moral principles with the principles of social prevention of crime such as poverty and unemployment so that criminal motives are taken away from criminals (Najafi Aberandabadi, 2003, 1208). A look at the ethical principles collected in the table makes it clear that ethical principles such as guidance and reform, science and effort, honesty, wisdom, justice and benevolence, and kindness, are all principles that can be applied in the direction of social prevention for Muslim users.

Staged prevention is another type of prevention that is divided into primary, secondary and tertiary prevention. In this study, we try to address its concept and function in the prevention of cybercrime and look at the principles of Islamic ethics which are compatible with this type of prevention.

The definition of primary prevention states: This type of prevention includes strategies that include social, economic, and other public policy areas which are used to influence crime situations and the root causes of the crime (Khosrowshahi, 2012, 12). Good manners in dealings, trustworthiness, honesty and sincerity are among the principles that can be generalized to examples of this type of prevention in terms of their function in preventing cybercrime. For example, we can mention the creation of videos and educational sites in which we have tried to

provide the necessary training to strengthen the nature of trustworthiness, honesty and sincerity and good manners in relationships and transactions through mosques, schools, books and other ways of transmitting these values, trying to apply primary prevention.

Another type of prevention is secondary prevention, which is a set of measures and actions related to groups and individuals who are more likely to be at risk of delinquency or deviant behaviors than other individuals. (Khosroshahi, 2009, 246), such as preventive measures for hackers or people who have the ability to infiltrate computer systems. Secondary prevention is prevention to neutralize dangerous situations, and in this type of prevention, the focus is on making changes in people, before they commit a crime which include anti-social or deviant behaviors such as wrongful and criminal activities on the Internet, creating immoral or criminal websites, and hacking sites (Ansari; Milani, 2016, 157-158).

Affection and kindness, knowledge and effort to enjoin what is good and forbid what is evil are among the moral principles of Islam that have the potential to be used as practical principles in relation to the secondary prevention of cybercrime.

Tertiary prevention, as the third type of step-by-step prevention, aims to monitor actions that prevent individuals from repeating the crime (Sarikhani; Soltani Bohloli, 2016, 142). Clear aspects of Islamic ethics such as repentance, forgiveness and human dignity are among this type of prevention, so by adhering to these two cases cybercriminals, officials and law enforcement will pursue the goals of this type of prevention and the purpose of Islam in establishing these principles.

Generalization of Islamic ethics principles to cyber ethics:

In addition to the general reasons given in the previous pages for creating an ethical feature and method specific to cyberspace, there are other reasons for this, such as the prevalence of such things as cyber invisibility, inherent anonymity, and exceptional flexibility in cyberspace (the ability to become what we can imagine) has made us more aware of the need for an ethical policy to prevent delinquency and victimization in cyberspace. As a Muslim user of cyberspace, there are many moral and spiritual values to which one must be faithful. We are not only expected to have the highest degree of honesty and integrity, but also to act responsibly, ethically and legally when accessing electronic private information. We must commit to protecting data, personal information and identities from unauthorized access or disclosure, and to respecting the ownership of information in all its forms.

The guidelines, which are based on Islamic moral principles and are recommended to cyberspace users, especially Muslims, to prevent and control crime, should be divided into two parts:

a. Fundamentals of Islamic principles related to cyberspace:

This is a set of principles for all human beings that apply in the real world as well as in cyberspace, like users. By maintaining, adhering to and applying these beliefs and values, we can see positive and low-cost effects in reducing and controlling crimes in cyberspace, which can be conceptually generalized to various types of prevention, especially social prevention:

1. Performing one's duty is an act of worship: Users and cyberspace professionals should know that doing their duty is an act of worship and God rewards them for their good deeds and punishes them for their abuse. Now, if these

people, who each have a different work and moral duty, do their duty of reporting crimes, protecting the privacy of people by building and installing security programs, etc., they have done both their worship and they have prevented possible crimes by applying the moral principles of Islam. In the holy Qur'an, God says: "So whoever does a good deed as much as the weight of a particle will be rewarded, and whoever has done as bad as the weight of a particle will be punished" (al-Zalzal Sura, verses 7 and 8).

2. Understanding and following the principles of Islamic ethics: Users and IT professionals should understand the standard Islamic ethics (based on the Qur'an and Sunnah) and consider it as the highest standard in their life and work.

3. The effect of remembering the Day of Judgment in preventing crime: Users and cyberspace experts should know that doing good deeds and producing useful knowledge, in life and after death on the Day of Judgment, will be rewarded by God. Remembering this, these people will always be careful about their actions so that they do not commit crimes.

4. Honest management: Managers and leaders in the field of cyberspace should be committed to an ethical-Islamic approach in managing the development and maintenance of hardware and software. They must show honesty and fairness in doing their job, if managers and employees put honesty into their work and build software or hardware safely based on that honesty, they can prevent crime.

B. Professional principles governing the ethics of cyberspace:

These set of ethical principles, presented by the American Computing Association, are accepted and used in most of the world and are addressed to cyberspace experts, and of course, there is no obstacle to extending it to other users, so

these principles are also called International Ethical Principles Governing Cyberspace. Therefore, in the following, these principles and their definitions will be examined separately and we will try to examine the compatibility of these principles with the moral principles of Islam. And by combining the two, we come to a series of Islamic moral instructions that can be called the Islamic Moral Principles of Cyberspace, which have an effective function in preventing and controlling crimes in this space. The professional principles outlined by this association are as follows: (Bernbach, 2009, 77-78):

1. Seek understanding first and then consent: Develop your empathetic ability to understand and internalize the consequences of your actions that may affect others.

2. Fair presentation: Keep the promises you make, as you point out.

3. Do not abuse your privilege of access to private information: IT professionals have unprecedented access to private information that requires a higher level of self-discipline.

4. Make every effort to prevent the illegal disclosure of private information: Ensuring the legitimacy, authorized access, and security of data that has been properly accessed is a fundamental concern and should be taken very seriously.

5 Use existing technology to protect private information: promoting and using technology developed by our peers to protect the data and tools which transmit it and using technologies such as encryption is part of our daily lives.

6. Efforts to improve the protection of private information: Avoid publishing and distributing information that is defective, inaccurate, erroneous or inappropriate. If you are aware of incorrect private information, or find information

that is not properly managed or secure, it is your responsibility to correct any incorrect, unprotected, or improperly managed private information. Or let someone who can do it know.

7. Do not use the work of others in your own name without the permission of the author: regardless of copyright issues; in order to use the work of others for professional or personal gain, it is unacceptable to use the work of others without the exclusive permission of the author, owner or copyright holder.

8. Staying steadfast in the direction of public policy and changes in social theory: Moral values are universally shaped by the concepts of justice, rights, harm, welfare and organizational fairness. Expand your moral reasoning by taking the time to understand these concepts to improve future decisions about moral dilemmas and conflicts.

9. Only have access to the information you need to complete your task: In order to complete your task, you do not have to view all the information available, however, it is up to you to decide what information is required. With that in mind, it's your responsibility to make sure you only use what you need.

10. Do not try to access computers or networks that are not licensed: As an IT user, you understand the importance of computer and network security, so trying to access computers and networks which are limited for the public is considered an immoral act.

11. Do not try to obtain information for the purpose of identity theft: because users expect people who have access to their information to be trustworthy and they want their privacy to be protected. The only exception to this instruction is to perform it for legally permitted purposes in order to enforce the law.

Identifying the ethical problems and challenges of cyberspace:

Thanks to cyberspace, it is now possible to engage in ethical or immoral activities and e-business anywhere in the world. Now the questions that can be raised here are : is it appropriate to monitor users' activities, such as emails and chat messages, electronically? Do you have to allow users to use their desktop computers for their personal business or to make copies of the software on their non-personal computers for personal use? Is it ethical to sell customer information extracted from transaction processing systems to other companies? Here are some examples of controversial ethical decisions you may have to make. Therefore, we need to take a closer look at ethical considerations in cyberspace. Identifying ethical issues affects how cyberspace is used in the organization, individuality, working conditions, privacy, crime, health, and solutions to social problems. Some ethical issues are discussed in the following section:

Access: What information does a person or organization with a right or privilege obtain, under what conditions and with what guarantee? Accessibility is currently one of the major concerns for implementing IT ethics.

Computer monitoring:

One of the most controversial ethical issues regarding the quality of work is computer monitoring. Computer surveillance has been criticized as a violation of users' privacy, as in many cases they do not know that they are being monitored or do not know how this collected information is being used. Because computer surveillance increases the stress on users and employees who have to work under constant electronic surveillance. In fact,

computer monitoring creates an "electrical exploitation workshop" in which employees are forced to work in harsh and unsuitable conditions, and companies, marketers, and Internet service providers engage users in a variety of ways (Sabernejad; Hosseinpour, 2018, 117).

Computer adaptation:

The unauthorized or incorrect use of personal information in computer adaptation is another threat to privacy. Another threat is the unauthorized matching of computer information about you that is extracted from sales transaction processing system databases and sold to information brokers or other companies.

Cybercrime:

Cybercrime is a threat posed by malicious or irresponsible actions by cyberspace users who take advantage of computer networks in our society and are possible in three ways: One is when the computer is the subject of crime. The second is when the computer is a tool of crime and the third is pure cyber crimes that are specific to this space, such as theft or cyber fraud (Jahanshiri, Hosseini, Ebrahimi, 2016, 15). So, this is a major challenge for the ethical use of cyberspace. Cybercrime poses a serious threat to the integrity, security and quality of business information systems. As a result, the development of effective security practices is becoming a top priority. Cybercrime include theft of money, services, software and data, destruction of data and software especially by computer viruses; malicious access to or hacking of the Internet or other computer networks, as well as a violation of privacy and other criminal offenses.

Private Issues:

Information technology technically and economically enables the collection, storage, integration, exchange and retrieval of data and information quickly and easily. This feature has a positive effect on the performance and usefulness of computer-based information systems. However, the power of information technology to store and retrieve information can have a negative impact on everyone's right to privacy. For example, confidential emails sent by employees are monitored by many companies. Each time you visit a site on the Internet, personal information about people is collected. Unauthorized use of such information could seriously damage your privacy. Mistakes in such databases can seriously damage a person's reputation.

Data alteration or theft:

Illegal alterations or theft of information is another form of cybercrime. In which financial information or identity information of individuals is stolen or altered by cybercriminals, which may cause problems for the person (Potter, 2012, 492).

Computer virus:

A computer virus usually enters a computer system through illegal copying or borrowing of copied software, or through network links that connect computer systems. Therefore, a computer virus or worm can spread the destruction among a large number of users. Viruses often destroy the contents of memory, hard disks, and other storage devices. As an action that we, the end users, should take, we should avoid using suspicious resources that have not been detected ant by antivirus software (Malekan; Salmani, 2012, 43-44).

Intellectual property:

It refers to intellectual innovations such as inventions, literary-artistic works, etc. (Mohammadzadeh, 2019, 66). As we know, unauthorized copying is illegal because the software has intellectual property that is protected by copyright law and user licensing agreement. Millions of dollars of software are illegally copied every year around the world. This phenomenon has a great impact on the software industry.

Pornography:

Pornography, which is considered an immoral crime in most societies, is considered a content-related crime and means images and content that are presented with the intention of arousing individuals sexually, and the number of Internet users is increasing day by day all over the world (Bai; Pourgharmani, 2009, 98).

Software plagiarism:

Computer programs and artistic or literary artifacts are valuable assets and are therefore intended to be used to steal computer systems. However, unauthorized copying of software or (literary) theft of software is also a major type of software theft and robbery (Momeni; Azizi, 2012, 45-46).

Health Issues:

Excessive use of cyberspace and computers can cause a variety of health problems. Excessive computer use has been associated with health problems such as job stress, arm and neck muscle injury, eye injury and fatigue, and exposure to radiation (Kakavand, 2009, 12-13). For example, monitoring employees' computers has been shown to be the main cause of job stress.

Conclusion

All human beings have a secondary life and identity, and that is their life and identity in cyberspace, which is expanding day by day. Major changes in the more advanced and diversified cyberspace cause many changes in social structures and our physical environments which are often unpredictable. Currently, the growing influence of cyberspace among the people, especially in Muslim countries, is quiet considerable. If we do not take seriously the fact that we are building a new environment in which future generations will live, we will have a problem. Although ethical and professional principles for IT users, including professionals, have been adopted by professional organizations and committees such as the American Computer Machinery Association as cited in the article, however, given the growing number of cybercrime cases, it turns out that IT users, including professionals, still face many ethical issues. Islamic sources (Holy Quran and Sunnah) provide high moral standards for individuals, communities and levels of the ummah (nation). Islamic ethics is stable, comprehensive, just and standard that is suitable for all nations and times; and when pursued, it leads to the creation of a moral community, followed by success in crime prevention. This article introduces the main steps of the roadmap as well as new principles for cyberspace users based on Islamic moral values. This effort can be useful in solving many issues related to the ethics of cyberspace users. This provides a good opportunity for IT users, especially Muslims, to understand and implement the standard and comprehensive moral values of their lives based on the moral principles of Islam, in order to succeed in preventing cybercrime.

Suggestions

1- Piety (fear of God) should be achieved as the main characteristic of a Muslim, so that he does not commit any crime that is harmful to others.

2- Tracking software can be installed to monitor and control the daily activities of IT users who use IT resources.

3- Different types of courses can be introduced based on Islamic ethics from elementary levels to higher education levels.

4-Understanding the fact that computer literacy and combining ethical issues with IT-related issues is a fundamental and essential skill in educational systems.

5- Creating a high level of awareness related to information security and issues related to cybercrime among home users, government and educational institutions, and in the private sector and among legal officers;

6- Increasing the exchange of information on information security and cybercrime at the regional and national levels;

7- Formation of policies and legal regulatory frameworks at the national level that are compatible with existing or developing legal instruments;

8- Establishing effective national and transnational mechanisms to prevent cybercrime and improve protection to identify and respond to cybercrime

9- Creating safe and secure environments for users, especially children and adolescents

10- Establishing effective mechanisms for identifying and responding to cybercrime at the national and regional

levels, including the creation of environments that help report cybercrime

11- Accepting and agreeing of the people with the instructions related to observing the ethical principles governing cyberspace

12- Promoting the power of people's understanding of the destructive nature of immoral issues in cyberspace and creating obstacles in the way of these issues

Resources:

1- Amini, Mohammad; Sharifzadeh, Fattah (2014), A Study of the Theoretical Relationship between Islamic Ethics and Organizational Framework Behavior, Ethics Research Journal, No. 25, pp. 151-172

2- Ansari, Jalal, Milani, Alireza, (2016), Critique of Iran's criminal policy against cyber fraud, criminal law and criminal policy, No. 1, pp. 145-164

4- Al-Tabatabai, Sayyed Mohammad Hussein (1417), Al-Mizan Fi Al-Tafsir Al-Quran, Teachers Association, Qom

5- Al-Tarihi, Fakhruddin, Bahrain Complex (unpublished)

6- Bai, Hossein Ali; Pourgharmani, Babak (2009), Jurisprudential and Legal Study of Pornography in Cyberspace, Islamic Law, No. 23, pp. 97-126

7- Pourshakibaei, Parivash; Jahani, Behzad (2017), Situation Prevention of Acid Spraying, Intelligence and Criminal Research, No. 1, pp. 33-54

8- Jahanshiri, Javad; Hosseini, Seyed Mohammad Reza; Ebrahimi, Ahmad (2015), Explaining the Preliminary Investigation Process in Cybercrime, No. 3, pp. 9-34

9- James Potter (2012), Recognition of Mass Media with Media Literacy Approach, translated by Amir

Yazdanian, Payam Azadi, Ali Tod, Tehran, Radio and Television Research Center, 1st Edition
10- Khorramshad, Mohammad Baqir, Head of Sadat, Sayyed Ibrahim (2011)
11- Khazaei, Zahra (2008), Ethics of Virtue and Religious Ethics, Ethics Research Journal, Vol. 1, pp. 83-97
12- Khosroshahi, Ghodratullah (2009), Secondary prevention of crime and deviation in the teachings of the Qur'an, Social Welfare, No. 34, pp. 245-274
13- Khosroshahi, Ghodratollah, Namamian, Peyman, Shokrbeigi, Alireza (2011), Crime Prevention in the Light of Religious Teachings, Journal of Cultural Engineering, No. 57 and 58, pp. 8-23
14- Dehghanzadeh, Sajjad; Ahmadian, Fatemeh (2016), A Comparative Study of the Principle of Pleasure in Charvake's Philosophy and Epicurean Philosophy, Philosophical-Theological Research, Vol. 69, pp. 143-167
15- Sarikhani, Adel; Soltani Bohloli, Maryam (2016), The Role of the Executive in Social Crime Prevention, Justice Law, No. 94, pp. 141 - 154
16- Sabernejad, Ali; Hosseinpour, Peri (2017), Legal Analysis of the Typology of Violation of Privacy in Cyberspace, Public Law Researches, Vol. 3, pp. 111-128
17-Feyz Kashani, Mohsen (1361), Al-Mahja Al-Bayda Fi Al-Tahdhib Al-Haya, edited by Ali Akbar Ghaffari, Press Institute, Qom
18- Qayyumi Muqari, Ahmad Ibn Muhammad, (1418 AH), Al-Misbah Al-Munir, Beirut, publisher of Maktab Al-Asriya, vol.
19- Kakavand Ghaleh Noei, Fatemeh (2009), Psychological and physical effects of computer and

Internet on children and adolescents, Report Journal, Vol. 215, pp. 12-13
20- Majlisi, Mohammad Baqir (1403 AH), Bihar Al-Anwar, Beirut, Dar Al-Ahya Al-Tarath Al-Arabi, vol. 68
21- Mohammadzadeh, Behnam (1397), Guarantees for the Protection of Intellectual Property in Law, Qanun Yar, No. 3, pp. 63-96
22- Malekan, Esfandiar; Salmani, Rasoul (2012), Computer viruses threaten the security of accounting information system, Accounting Research, Vol. 7, pp. 39-50
23- Momeni, Negar; Azizi, Sirus (2012), plagiarism (scientific) and the role of language tools in its identification and analysis, Detective Quarterly, Vol. 20, pp. 44-69
24- Najafi Aberandabad, Ali Hossein (2003). Criminology course lectures. Master's degree course in Qom Higher Education Complex, compiled by Mehdi Seyedzadeh
25- Ahn, Katherin (2006), A Study on the Methodology of Information Ethics Education in Youth, IJCSNS International Journal of Computer Science and Network Security, vol6, pp91-96
26- Berenbach, Brian (2009), Professional and Ethical Dilemmas in Software Engineering, Georgia Institute of Computer Technology, vol 42, pp 74-80
27- Couger, Daniel (1989), Preparing IS students to deal with ethical issues. MIS Quarterly journal, vol 13, pp-211-218
28- Froehlich, Thomas, (2000), Rafael Capurro and the Challenge of Information Ethics, The International Information & Library Review, Volume 32, Pp 277-282

29- Gilbert, Jackie & Bette Ann, Stead, (2001), Ethical issues in electronic commerce, Journal of Business Ethics, vol34, pp75-85
30- Hilliard, Robert. L & C, Keith Michael (2007), Dirty Discourse: Sex and Indecency in Broadcasting, Hoboken, New Jersey, published by John Wiley & Sons
31- Iacovino, Livia (2013), Ethical Principles and Information Professionals: Theory, Practice and Education, Australian Academic & Research Libraries,vol33 ,pp57-74
32- Kenneally, Erin, Bailey ,Michael, Maughan, Douglas (2010),A Framework for Understanding and Applying Ethical Principles in Network andSecurity Research,International Conference on Financial Cryptography and Data Security, Spain
33- Kimball , Marshall, (1999), Has technology introduced new ethical problems?, Journal of Business Ethics, VOL 19,PP 81–903
34- Leicester ,Nicola, (2016), Ethics in the IT Profession: Does a Code of Ethics have an Effect on Professional Behavior?, Research Project in Information Management, wellington,Victoria university of wellington
35- lourdu, vesna.j & Niveditha ,Daniel(2012), Ethics in cyberspace - a philosophical approach, International Journal of Advancements in Research & Technology, Volume 1,pp58-62.
36- Maghaireh, Alaeldin(2008), Shariah Law and Cyber-Sectarian Conflict: How can Islamic Criminal Law respond to cybercrime?, International Journal of Cyber Criminology, Vol 2 (2),pp 337–345

37- Peterson, Dane .K (2002), Computer ethics: The influence of guidelines and universal moral beliefs, Information Technology & People , vol15, pp346-361
38- Ronald, Sims؛ Brinkmann, Johannes(2003),Enron ethics (or culture matters more than codes),Journal of Business Ethics, vol 45, pp-243-256.