Eksplorium *p*-ISSN 0854-1418

Volume 45 No. 2, November 2024: 17–29 *e*-ISSN 2503-426X

Criminal Policy of the Islamic Republic of Iran in the Face of Cybercrime Content Filtering with Emphasis on Economic Issues

Yaser Ansari[1]; Seyyed Mohammad Reza Mousavi Fard[2]*; Marjan Neghi Mokhlesabadi[3], Sajjad Akhtari[4], Mojtaba Ghaffari[5]

Article Received: 17 Sep 2024, Revised: 25 Oct 2024, Accepted: 05 Nov 2024

Abstract: The diverse and new forms of crimes at the domestic and international levels are due to the emergence of technical and technological advances in the field of computers, which has made it easier for criminals to commit crimes in many cases. Naturally, in the field of cybercrime, we are faced with a very wide range of crimes, which itself requires the necessity of appropriate policymaking and a safe and active strategy in the scale of crimes in this field. The sensitivity of the matter increases when we witness cybercrimes in the micro and macro economic areas of a society, because undoubtedly its goal is to disrupt the balance and equilibrium of the economic system and, consequently, to violate the rights of individuals and ultimately to damage the economy of small domestic communities such as the family, which in itself is the basis for a significant range of other crimes. This article examines the basics and concepts of computer crimes and filtering, as well as criminal policy towards these crimes, and shows how to prevent them. What has been clarified in this article is that today there is no doubt that the development and expansion of the Internet, as well as the use of this new communication tool, requires a codified and coherent legal system. Filtering cyberspace as a measure to make this ecosystem healthy, has been a constant pillar of the governance policies of the Islamic Republic of Iran in order to ensure the freedom of this new media, prevent possible abuse of freedom of expression, and assure the people that their access and use of Internet media will be cheap, safe, and sustainable. While the economy-oriented is directly based on the acquisition, production, distribution and application of knowledge in all economic activities. Currently, achieving economy-oriented knowledge is a requirement of all countries in the world. The Internet is also one of the world's current technologies, so there is a specific policy in this regard in the form of the Computer Crimes Law and specific laws.

Keywords: Criminal policy, cyber criminal content, economic issues.

INTRODUCTION

The developments related to the information and communication technology revolution have provided the basis for a profound impact on the socio-economic formation of societies and the reshaping of the international political economy system. The transformation resulting from the digital revolution in the global system is transmitted to the five continents with intensity and weakness and changes. The direction and direction of these changes are determined by the cultural, political, economic and security systems of countries in their interaction with the global system. (Dehghani and Pourahmadi Meybodi, 1402: 3)

Information and communication technology has enabled the emergence of a network society that offers new definitions of human identities and societies and its main context is information and the electronic communication system. In such a way that in advanced societies, its use is considered a necessity, as this makes the world look like a village and its members can easily communicate with each other wherever they are. Therefore, the desire and enthusiasm to use computers and the Internet and benefit from its benefits is a global tendency. Although it provides opportunities for community participation in many areas, it also creates conditions and grounds for the emergence of new criminal phenomena that threaten the security and privacy of society and individuals. Today, this achievement has made it much more likely for thieves to succeed using a computer than a weapon, and perhaps tomorrow's terrorists will be able to inflict more security damage on individuals using a keyboard instead of a bomb. In particular, people prone to crime have a potential factor in the spread of these crimes by using this technology. In general, what is called cybercrime today is the growing process of this type of crime, which can be considered a factor in causing damage to social security and undermining national security.

Unlike many other terms that express the concept of a field of study with a specific subject and framework, the term criminal policy is mixed with an inherent ambiguity that places its limits and content as a scientific field in a halo of ambiguity, so that the diversity of interpretations of this term is visible even among legal and criminological thinkers and writers, such that some have a narrow interpretation of criminal policy and some have a broad interpretation. (Sadeghi, Abbasi and Ghasemi, 1400: 2)

Criminal policy refers to the set of methods used by the government and society to prevent and control the criminal phenomenon, which indicates the type of attitude of each government system towards crime, criminals, punishment, and in a way indicates the ideology that governs society. Criminal policy at three levels: legislative, executive, and judicial, attempts to respond appropriately to crime and deviance by employing a variety of criminal and non-criminal methods.

The components of the narrow concept of criminal policy can be listed as follows:

a) Measures and actions that are mainly coercive and punitive are defined, determined, and implemented through the criminal system to deal with criminals; b) These tools have an official (governmental) aspect, meaning they are determined and implemented solely by the general powers of government (courts, police, prisons, etc.); c) The measures used only deal with fighting crime, and other deviant behaviors, despite their social and moral ugliness, are outside the scope of this definition due to the lack of a guarantee of criminal enforcement; d) Crime prevention in this definition is achieved only through repression and criminal enforcement, and specific preventive measures have no place in it (Zargari, 2014: 221). Other thinkers such as the German von List in (1889), the French Couch in (1905), and the Dandy-Yu-de-Waber in (1938), following Feuerbach's perspective, made this way of thinking dominant in the realm of criminology until the middle years of the twentieth century. Against the narrow concept of criminal policy, some thinkers not only do not consider the fight against crime prevention and management to be limited to the framework of criminal law, but also consider other legal systems and the social system to be involved in this matter. Meanwhile, some, by introducing the concept of deviation or deviance alongside crime, consider both elements worthy of the attention of the board or body of society and believe that the criminal phenomenon should be organized and ultimately controlled with the cooperation of all government institutions and non-governmental organizations. The standard-bearer of this view should be Marc Ansel. In one of his articles in 1975, he introduced criminal policy as both the science of observation and study and the art of technique or principled and systematic strategy of anti-criminal response. Following Ansel's view, another French scientist named Miriam Delmas Marty, who can actually be considered the continuation of Ansel's scientific approach and thought, presented a more comprehensive definition in 1983 from which the absolutely broad concept of criminal policy can be obtained. In Marty's view, criminal policy is a set of methods that the social body uses to organize the response to the criminal phenomenon, that is, crime and deviance. According to this definition, the criminal response to the criminal phenomenon as an expression of reward and punishment is considered one of the diverse and diverse responses of the state to this behavior. (Laserge, 2003: 10)

Therefore, according to this interpretation, in addition to the fact that responses to the criminal phenomenon include criminal types, it also includes other legal systems such as administrative, civil and disciplinary. On the other hand, the state, along with civil society, organizes and implements criminal policy. The criminal phenomenon in this perspective includes both concepts of crime and deviance, and finally, criminal policy in this perspective includes not only repressive criminal responses (reactive) but also specific preventive (active) actions and responses against crime and deviance. One of the important issues in the realm of criminal policy is the issue of how to receive and accept criminal policy, or in other words, the feasibility and effectiveness of a strategy or strategy, in simpler terms, the implementation method that may be preventive or repressive.

Accordingly, this classification of criminal policy represents that three levels of criminal policy can be distinguished from each other: 1. Legislative criminal policy, 2. Executive-judicial criminal policy, 3. Participatory criminal policy. (Najafi Abrandabadi, 2011: 32)

Given all these explanations and as the title suggests, the main issue and topic of this project is the study of criminal data filtering on the Internet from the perspective of economic-based criminal policy. In this way, we have examined a number of the mentioned levels of criminal policy in this work in the context of cyberspace and, in fact, we have sought to find examples of implementing criminal data filtering from the perspective of economic-based criminal policy regarding cyberspace. In other words, the issues under discussion are, firstly, what measures the Iranian legislator and the ruling powers have devised to combat and prevent cybercrimes from the perspective of the constitution and subordinate laws such as resolutions and regulations, and secondly, what kind of executive-judicial criminal policy the country's executive branch has put forward in order to be able to fulfill its duty of eradicating and preventing crimes in these types of spaces.

Definition of Cyber Economic Crime

Despite the inexorable prevalence of cyber economic crimes in today's societies, there is no precise and comprehensive definition of this type of crime, and the various existing definitions have been explained based on the characteristics of these types of crimes. Therefore, special attention should be paid to the three main characteristics of cyber economic crimes, around which most definitions have been explained. These characteristics are:

- Technological complexity (numerous ambiguities and difficulty in recognizing the specialized and technical dimensions of cyber economic crimes due to the complexity of cyberspace).

- Diversity and variety of cyber economic crimes (due to the evolution and development of cyberspace).

- The ability to mystify cyber economic crimes.

However, given the need for a precise explanation and definition of the crimes known as cyber economic crimes, international documents, both guiding and binding, and international and national legislative authorities of countries, each have provided different definitions of these crimes according to the existing needs and threats. In general, in a comprehensive and preventive definition, cyber economic crimes can be described as follows: "Any criminal act or omission that is carried out with the aim of illicit financial gain or related matters through a computer and any similar tool in the context of cyberspace and information networks is a cyber economic crime." It is noteworthy that the aforementioned definition is only one example of the numerous definitions available, which, according to the researcher of this study (me), is comprehensive of other definitions. However, the reliability of definitions of examples of cyber economic crimes such as computer theft and cyber fraud, etc. is very effective and is the subject of this study.

Characteristics of Cyber Economic Crimes

Cyber economic crimes, like other crimes in the field of cyberspace, share many common characteristics. For example, in such crimes, the time and place of committing the crime are not relevant, and they can be committed at any time of the day and in any place where there is minimal ability to connect to a computer network. These crimes are also much more widespread, faster, and at the same time less dangerous than similar non-computer crimes. In other words, the volume and frequency of fraud or theft is much greater and occurs in a very short time, while the security of the thief or fraudster is much less threatened by regulatory and law enforcement authorities. In addition to the above, in such crimes, the true identity of the perpetrator is usually not disclosed, and in most cases, the criminal intentionally or unintentionally involves intermediaries in criminal operations in order to reduce the possibility of being traced.

CHARACTERISTICS OF CYBERCRIMES

Regarding the previous discussion, based on the existing assets and the definition of crime in the legal perspective of the Islamic Republic of Iran, it can be said that a crime is any act or omission that is punishable by law. Therefore, cybercrime can be implicitly defined as any act or omission that occurs in cyberspace and is punishable by law. (Sobhkiz, 2012,:27) However, such crimes, due to the environment in which they are committed, have distinctive features and characteristics that are far more attractive to criminals. Undoubtedly, the cyber environment provides facilitating benefits that make it much easier to use, and this is why criminals in the present era prefer criminal activity in cyberspace to traditional crimes. In general, the characteristics of this information service include: wide access area, speed of access, ease of access, variety of applications and economy (Danaei, 2009: 171-172.) which we will briefly discuss below:

- Possibility of anonymity and identity forgery

Among the unique characteristics of this space is the possibility of anonymity and being unknown in it. In other words, anonymity is one of the principles governing crimes in the virtual world. (Javan Jafari, 2010: 176) Failure to identify the perpetrator and the lack of reliable identification create unjustifiable security in reality and in the eyes of criminals, which has no result other than the audacity of the aforementioned and the increase in the number of computer crimes, and consequently, significant losses for every society.

- Violation of time and space limitations

As a result of the amazing violation of the time and space pillar in conventional human activities, as cyberspace spread throughout the world, the violation of the time and space dimension of committing crimes in the form of computer crimes was predictable. This surprise occurred due to the remarkable growth of information and electronic communication technologies, and the proposition of time and space in human daily activities underwent changes. Since then, a fraudulent transaction can be committed from a distance of thousands of miles and in a fraction of a thousandth of a second, and at the same time, a harasser can target his victim with his mocking speech from a great distance and in real life. (Williams, 2012: 49-50)

- Extent, diversity and multiplicity of opportunities

Technologies have long been at the service of human comfort and progress. Now, what has the technological space of cyberspace helped humanity? Undoubtedly, the cyberspace is a powerful tool for promoting multiple social, scientific, and cultural dimensions. This space has increased public awareness along with the ability to monitor specifically and publicly, and has become a barrier to the commission of many crimes by publishing information instantly. However, it has also had and continues to have significant problems. Due to its effective features, cyberspace has provided a safe, private, and comfortable environment for committing crimes, especially cybereconomic crimes and crimes against morality and chastity. This opportunity, which, along with other related facilities and privileges, has provided a privileged position for criminals, tempts even individuals who are committed to observing social norms to express their unconscious norm-violating instincts. Therefore, some believe that this space is a clear example of a safe haven for norm-violators. (Jalali Farahani, 2010: 17) Cyberspace is a relatively free space that cannot be defined by any specific limits or boundaries. Naturally, criminals understand this well and use it to advance their wrong goals. Today, the abundance of opportunities to commit crimes and the expansion of the dimensions of crimes due to the availability of the requirements and the lack of obstacles to committing them have become the main concern of experts, which cannot be corrected except by reducing the opportunities. However, this reduction in opportunities must be done very intelligently so as not to harm the useful principle and the quality and public and private benefits of cyberspace.

- Increased speed and ease of committing

Among other characteristics of cyberspace in the field of committing crimes, we can mention the ease and speed of committing them. Specifically, traditional criminals face a lengthy process in committing crimes. Also, in terms of committing crimes, one of the factors that slows down the occurrence of criminal phenomena in the real world is the need for spatial consensus between the three pillars of crime realization, namely the criminal, the target of the crime, and the place where the crime was committed. However, the structure of cyberspace is such that spatial proximity between the three above elements is not necessary. (Javan Jafari, 2010: 176) Today, cyberspace, due to its characteristics, has provided a platform for criminals to implement their criminal goals with minimal time and ease. This speed and ease sometimes accomplishes the crime in the form of a simple click. For example, in committing a crime of fraud in cyberspace, it is not necessary to fulfill the specific elements and elements of this crime in the real world, therefore, specific fraudulent maneuvers and face-to-face interactions have given way to pressing just a few clicks and performing mundane operations, which unfortunately results in an increase in the number of computer crimes. (Belfer Center, 220:384)

- International Nature (Transborder)

The transnational or international scope of cyberspace is one of the most important properties of this space that has fascinated criminals with its capabilities. According to evidence, virtual networks were previously used locally or at most regionally, and there was no evidence of the network's global and international reach, but with the help of wireless and wired systems, such as satellite networks or fiber optic lines, this possibility has been made possible. (Jalali Farahani, 2005: 142) Ultimately, activities under an international network will have international effects, and accordingly, committing a crime in this context can have transnational and international effects.

- Weakness of supervision and control

The lack of adequate supervision and the lack and inadequacy of deterrents in cyberspace give criminals the courage to freely carry out their criminal acts in this space. Criminals in this space find the field devoid of order and appropriate law enforcement forces and commit criminal acts. The current world creates a situation where users, free from any supervision and control, are busy with computers and cyberspace in their privacy and easily fall into an unbridled space in which there is no trace of government and social factors restricting freedom. (Aalipour, 2011: 99) It should be noted that effective strategy and necessary policy-making in the field of cyberspace are largely beyond the control of governments, including the Islamic Republic of Iran. This situation is while, according to some experts, freedom of action is one of the most important requirements of the cyber environment, but based on the principle of applying international rules within countries, these requirements should not contradict and violate the values of the system and internal regulations, in which case they deserve serious confrontation. The important point is that monitoring and controlling cyberspace must be applied with special delicacy and intelligence so that it does not lead to public dissatisfaction due to disproportionate measures. In any case, this space has no private or government owner, is not subject to a global regulation, and there is no public legislator in it. All these things in the cyber environment, such as the lack of precise regulations in the virtual world, have caused it to be interpreted as the "new wild west" (Javan Jafari, 2010: 171)

- Low cost

In computer crimes, we are faced with a decrease in the costs of committing a crime due to the relative increase in the effects of the crime. This, along with the other mentioned issues, has increased the number of computer crimes and makes it more difficult and complex to deal with. The most important and most widely used hardware for committing crimes in cyberspace are, respectively, various types of computers and smartphones, mobile phones, in addition to a telephone line for connecting and using the Internet. What is noteworthy is that the low cost of committing the relevant crimes somehow leads to a higher number of crimes, which consequently exacerbates the shortcomings and limitations of financial and human resources for the criminal justice system. (Nicola Lucchi, 218: 359) For example, in 2002, a Filipino user caused significant damage of about 10 billion dollars by systematically spreading a virus called "I love you" and disrupted many computers around the world. (503Ramachander, 2021:) This action of his took place in the shortest possible time and at the lowest cost, but it had significant effects on the global community.

- The high number of black figures

The high number of black figures in the field of computer crimes is due to two reasons. One is that, for the reasons mentioned above, it is fundamentally much more difficult to detect types of cybercrime than types of traditional crime. Furthermore, reputable companies and institutions are reluctant to disclose such crimes, which confirm the instability and insecurity of their economic activities, because this disclosure tarnishes the reputation of these commercial and industrial enterprises, which are based on customer trust. As a result, the two factors mentioned can lead to an increase in the number of crimes in cyberspace.

Also, undoubtedly, one of the effects of a high number of crimes is the reduction of the deterrent effect of the prescribed penalties, because a high number of crimes means a reduction in the probability of arrest and punishment. In the economic analysis of crime and punishment and within the framework of rational choice theory, as the probability of arrest and, as a result, the execution of punishment decreases, the deterrent effect of existing legal penalties decreases and, as a result, the probability of committing a crime increases.

- Automaticity

The automation of the crime does not apply to all types of computer crimes, but this category has a significant share in the statistics of computer crimes. Sometimes the design of a software automation system leads to a range of crimes such as theft of information and property in cyberspace. In recent years, in a part of computer crimes, we have encountered online systems that have acted as agents of botnets (networks of criminal robots under the control of computer criminals). The way these botnets work is, for example, that you receive an interesting message in a messenger from a friend and click on the email address sent, after which the system and software ask you to install a specific software or extension to run that program or update it in order to watch your favorite video. After you click, a malware is actually installed on your computer and, according to the program's command, systematically sends all the information on the device to the program designers. In this way, criminals gain access to your information system online, continuously, and automatically without the need for any other actions. A hacker can also insert these dangerous robots into multiple and different computers and form a botnet network. Such networks, which are generally in the hands of hackers, can automatically send and receive a significant amount of information and commands against the will of users. (Karmi, 2015: 83)

- Intangibility and internality of the crime

In the field of cybercrime, in many cases we are faced with crimes that will not attract attention at the moment, and for this reason, the prosecution and detection authority will not deal with it due to the lack of recognition and awareness of the crime until statistics are found. This feature can be referred to as the intangibility of cybercrimes. Among the crimes subject to the characteristic of intangibility, we can mention examples in the field of crimes of information theft, espionage, or even petty thefts and cyber violations that occur in large numbers, although they may never be noticed and discovered.

Another feature of computer crimes is the internality of these crimes in most cases. Internality refers to a crime when the perpetrator attempts to commit a crime in a group through connection and membership in that group. For example, in the field of traditional crimes, it is possible that a crime is committed through the instigation or supervision of individuals who have an effective relationship with the subject of the crime, such as the crime of embezzlement, which requires the existence of an employment relationship between the criminal and the institution in question, and consequently, this criminal, through his information and authority, attempts to commit the crime of theft or breach of trust. However, given the information and knowledge of the criminals about the subject and the environment of committing the crime, which is due to the trust of the institution in the criminal, we generally witness extensive dimensions and far more harmful effects in this type of crime. For this reason, the legislator has considered this situation and similar situations to be subject to an aggravated criminal quality and has foreseen far more severe punishment for its perpetrators, such as what is seen in embezzlement compared to breach of trust and theft by employees compared to simple theft in the Islamic Penal Code. However, this problem is observed in a more severe form in computer crimes. Employees, contractors, consultants, partners, and associates of companies are the main perpetrators of crimes against an organization or company, and it is not easy to distinguish them from external perpetrators.

Types of Cybercrimes

The legislator of the Islamic Republic of Iran, by establishing and approving a set of special rules called the Cybercrimes Law, has implicitly divided computer crimes into different types. This division is determined based on the qualities of punishment and the type of crime committed and has been compiled under the protection of the Islamic Penal Code.

Types of cybercrimes in Iran, according to Articles 1 to 25 of the Cybercrimes Law, or in other words, Articles 729 to 753 of the Islamic Penal Code, have been enumerated in seven chapters, which include:

Crimes against the confidentiality of data and computer and telecommunications systems, such as unauthorized access, unauthorized eavesdropping, and computer espionage, etc.

Crimes against the accuracy and integrity of data and computer and telecommunications systems, such as computer forgery, destruction and disruption of data or computer and telecommunications systems, etc.

Computer-related theft and fraud

Crimes against public morality and morality, such as publishing, distributing, or trading in obscene content using computer systems or data carriers

Defamation and spreading lies

Other crimes, such as producing, publishing, or distributing data solely for the purpose of committing crimes Computers are used and other crimes specified in various articles

By carefully separating the crimes in this area, it seems that this group of crimes includes two groups: computer crimes and telecommunications crimes. In addition, the separation of these two groups has been duly considered both in the Cybercrime Convention adopted in 2001, which is considered the most important international document in the field of cybercrime, and in the Computer Crimes Law adopted in 1388.

Based on the separation made in the Cybercrime Convention, these crimes can be placed in four categories, which are:

❖ Crimes against the confidentiality, integrity and availability of computer systems and data: These crimes are mentioned in Articles 2 to 6 of the aforementioned convention, which include unauthorized access, unauthorized eavesdropping, data disruption, and misuse of devices, respectively.

❖ Computer-related crimes: Articles 7 and 8 of the Cybercrime Convention refer to two crimes of forgery and fraud related to copyright, respectively.

❖ Content-related crimes: Article 9 of the Convention refers to crimes related to child pornography, which are naturally considered crimes related to the content of computer data. Of course, Article 3 of the Additional Protocol to the Cybercrime Convention in 2003 also criminalizes the dissemination of racist and xenophobic content through computer systems, which can be considered a cybercrime related to content. (Jalali Farahani, 2010: 152)

❖ Crimes related to copyright infringement and related rights: Article 10 of the Convention refers to crimes related to the infringement of intellectual property rights, including copyright.

The impact of technology on economic crimes Today, in line with the increasing growth of e-commerce platforms in the world, and especially in Iran, we are faced with the component of the computer economy and its progress. It seems desirable for any society to have the necessary cultural, economic, social and security platforms ready and always ready to be present in the

Islamic Penal Code, Articles 656-673 and the Law on Increasing Punishment for Perpetrators of Bribery, Embezzlement and Fraud, approved in 1988 by the Expediency Council, in the scope of global e-commerce. However, ignoring the weaknesses and threats arising from cyber economic crimes in this area can turn this phenomenon into an unpleasant phenomenon for a society. Numerous studies show that fraud, security breaches and privacy violations are still the main scourge of the growth of e-commerce. Today, most economic crimes have a computer version. This type of crime provides criminals with more opportunities with greater efficiency and fewer risks. For example, websites can be forged, misused, and defrauded. Electronic payment systems can also be compromised through criminal approaches, and electronic funds can be transferred to provide a suitable platform for theft or quick money laundering. This situation has led to the loss of public trust in this system and has led to increased concerns and serious demands for computer economic security. Therefore, people do not show sufficient interest in fully accepting electronic commerce due to these concerns. This approach consequently prevents the integration of commerce and cyberspace, and thus society is deprived of the significant benefits of the electronic commerce system. However, it does not seem logical to sacrifice the trust of society for these benefits. It seems that a balance should be established so that over time and according to the plan, we can witness the electronicization of the country's economic and commercial space.

CONCLUSION

The peculiarity and feature of the Internet and the ease of publishing content and information, and in addition, the ease of accessing various types of information on the web, including text, audio, images, and various graphic data, have increased to such an extent that in some cases, information containing harmful content is also published on the web, which has paved the way for various abuses. In other words, the Internet, along with all its useful services and applications, as well as its significant impact on improving human lives, can become a platform for the abuse of freedom and illegal actions of criminals and evil individuals. Promoting racism and violence, encouraging membership in terrorist groups and training suicide bombers, publishing images of child sexual abuse, pornography and promoting unconventional methods of sexual relations (homosexuality and violence in sexual relations), widespread violations of intellectual property rights, online gambling, and ... are examples of harmful and illegal activities that are taking place on the Internet today.

There are solutions to make cyberspace healthy, and just as it is necessary to have a healthy and safe society, it is necessary to establish laws and disciplinary and legal controls, so that different social groups and classes can benefit from the facilities of cyberspace without being harmed; and to prevent the aforementioned illegal and harmful actions and minimize their effects, measures are taken by responsible institutions at various national and international levels. One of these measures is Internet filtering; the purpose of filtering, or in other words, Internet filtering, is to create restrictions on access to content or websites containing illegal or harmful materials.

Although the main reasons for Internet filtering are mostly social standards, ethical issues, or ensuring national security, its examples and extent are by no means agreed upon by everyone, and there is no common international standard proposed by an international organization in this regard. In these circumstances, each country formulates policies and plans for filtering based on its own political and cultural points of view.

The main reasons for filtering the Internet in different countries can be grouped into four general categories: political issues, social issues, security issues, and ethical issues. What makes each country fundamentally different for filtering is the fundamental values considered in each category in those countries. The basis for using filtering is to protect individuals' privacy and observe the principle of freedom of communication.

With a detailed understanding of the state of the Internet, there is no doubt about filtering its illegal and harmful content; however, given the impact of the Internet in ensuring the right to freedom of expression and free access to news and information, it is necessary to identify and apply principles and rules for filtering Internet information bases (filtering), including the seven principles of Internet freedom, minimal government intervention, legality, transparency, the possibility of litigation, intelligence, and education based on human rights documents, UNESCO resolutions, and Council of Europe recommendations, as well as the experiences of leading countries in the field of communications law and the Iranian legal system.

In the Freedom of Information and Right to Access to Information Act, information such as foreign relations, national security, issues related to the commercial and business activities of the state, government, or individuals, as well as the personal affairs of individuals, are usually excluded.

Unauthorized access, meaning unauthorized (illegal) access to content stored or being processed in one or more systems, telecommunications, or networks, is criminalized in Article 2 of the Cybercrime Act, and since the Computer Crimes Act is designated as an independent chapter of the Islamic Penal Code, Article 48 of the Criminal Code should also be referred to regarding the repeated offense of unauthorized access. Articles 136 to 138 of the Islamic Penal Code are also dedicated to repeated offenses.

The basis and objectives of filtering policy are similar in terms of examples and definitions; for example, one of the main bases and reasons for filtering is to protect privacy, which this concept differs according to the legal systems of Iran and the European Union. Filtering implemented by governments can, in addition to ensuring the security of families and children in cyberspace, prevent destructive or terrorist activities, provide the necessary levers to deal with any kind of sabotage in the cyber world, eliminate the tension created by government opponents, and overall, create a safe and peaceful atmosphere in society.

Legal filtering of Internet data content has various types based on content and social categories; for example, filtering types based on content are divided into political content, social content, conflict and security, and Internet tools. Filtering based on social categories also includes job filtering, gender filtering, age filtering, and moral filtering.

According to Note 1 of Article 749 of the Computer Crimes Chapter of the Islamic Penal Code in the Islamic Republic of Iran, filtering of cyberspace is considered as a last resort (in case of non-responsiveness to the prohibition of evil and failure to remove the content by the website owner).

The right to free access to information is a right that is considered essential for the survival of democracy in a society and to guarantee the sovereignty of the people. This right has been recognized in many international documents and conventions, and comprehensive definitions have been provided about it. In our country, the "Law on the Publication and Free Access to Information" was also passed in 2009.

The current mechanism for filtering cyberspace in Iran is based on blocking websites based on domain names, which does not have the ability to separate useful and immoral parts of the website. This causes even useful and non-criminal content to be inaccessible to users in some cases. In Chapter 749 of the Computer Crimes Chapter of the Islamic Penal Code and all its notes, the word filtering is mentioned along with the phrase “content.” In other words, “content filtering” and not filtering all website information. According to Article 19, Paragraph 43 of the Human Rights Code, filtering should only include that part of the website that contains criminal content and not the entire website, which is reflected in the choice of the name “Criminal Content Committee” and the inclusion of the phrase “content.” Unauthorized access, meaning unauthorized (illegal) access to content stored or being processed in one or more systems, telecommunications, or networks, is criminalized in Article 2 of the Iranian Computer Crimes Law, and since the Computer Crimes Law is designated as an independent chapter of the Islamic Penal Code, Article 48 of the Criminal Code should also be referred to regarding the repeated offense of unauthorized access. Articles 136 to 138 of the Islamic Penal Code are also dedicated to repeated offenses.

Also, blocking, meaning that the connection to the entire content is cut off by the relevant server and the possibility of anyone accessing that information is completely eliminated. Accordingly, blog service providers are also obliged to block specific blogs as soon as they are notified of the cases; this is a legal obligation.

In general, a series of specific monitoring and control measures are taken on the activities and performance of the media, as follows:

Control of media content and themes for political, cultural and ethical reasons, industrial or economic reasons. The characteristics and themes of the media that may be taken to justify the application of media control are as follows: In order to have political effects (stopping some political actions), moral and cultural and emotional, it is subject to greater control.

Regarding the authority of governments to intervene in the Internet and filtering such as issuing licenses, formulating laws and regulations, monitoring and control, there are general attitudes and perspectives, including government monopoly, government cooperation with non-governmental and independent institutions, and delegating all affairs and powers to non-governmental institutions, and the application of each of these perspectives leads to the adoption of specific and different methods and measures. At the European Union level, voluntary filtering is used to a significant extent as a way to limit government intervention and involve other Internet actors, as well as filtering through voluntary self-regulation by search engines. However, what is common between the two legal systems of Iran and the European Union in their general policies on the subject is that the principle of minimal government intervention is established in the Internet, as in other media. Internet filtering, as a restriction on freedom of expression, must be carried out in accordance with the law, while usually the examples of filtering are formulated by an independent institution and are publicly announced before implementation. This action is in a way derived from the principle of legality of crimes and punishments in criminal law.

The scope of cybercrime has overshadowed human life more than ever before and has made humanity dependent on it in some way. The unique advantages of cyberspace are the reason why economic and other activists have migrated to this space. These days, every child and teenager can find a tool to connect to the virtual network, but the culture of using and being in this space is rarely found. Therefore, the biggest and most important scourge of this space can be considered the ignorance and lack of knowledge of users about the operational space. Also, the shortcomings of this space in terms of security and reliability, etc. should not be hidden from view. Therefore, it seems that if the existing shortcomings are eliminated, we can witness more prosperity in all parts and dimensions with the support of proper education and identification of the neglected dimensions and capacities of this space. This is a healing prescription for solving the problem of unemployment and expanding national and international trade relations and, consequently, the growth of exports. The progress of countries such as China and the United States in this regard cannot be hidden, and large successful sites in the field of online sales can be considered leaders in realizing this ideal. Along with culture and education, what creates the stage for technological prosperity in the country's economy is the quality of infrastructure and the context of activities. The realization of a coherent and at the same time dynamic system requires a dynamic, understandable, practical and secure space. Naturally, cyberspace, in accordance with its universal nature, has an acceptable quality in most of its effective quality components and is in accordance with global standards. In the meantime, there are also duties on the responsibility of the internal systems of each country. The fulfillment of these duties is achieved correctly and with quality when international interactions are achieved alongside correct domestic and foreign policymaking, but an appropriate policy becomes effective when it experiences correct and high-quality implementation. Although the Islamic Republic of Iran has not been among the leading countries and major players in the global community in this regard, it has an acceptable and at the same time progressive position in the region due to the effective policies and actions implemented in recent years. It seems that what is preventing the urgent promotion of the Islamic Republic of Iran in the field of cyberspace is partly related to the failure in international interactions and relations resulting from the cruel sanctions of hostile countries and partly to defective and incomplete domestic policies. Perhaps the lack of up-to-date and effective laws in the field of combating cyberspace crimes can be considered the most effective factor in the failures of the cyberspace field, because it has turned this space, which is a suitable and suitable platform for beneficial economic activities, into a haven for criminals. Undoubtedly, the lack of effective criminal laws regarding emerging and novel crimes is a challenge that government systems and legislation have been facing for a long time. Cybercrimes are of interest in this regard, given the rapid development of information and communication technology and the short history of criminology in this field. Given their inherent characteristics such as the ease of committing the crime, the large number of victims, anonymity, and the young age of most of the criminals, these crimes require specific criminology principles in addition to general principles. The Islamic Penal Code has provided laws specifically for computer crimes since 2009, but today, given the rapid development of information and communication technology, many shortcomings can be found in the aforementioned laws. These shortcomings have led to a lack of sufficient deterrence and will lead to more cybercriminals being acquitted than before. Currently, we are clearly witnessing the rapid growth of economic crimes in cyberspace, and this problem not only reflects an inappropriate image of our country in the international arena, but has also made domestic users at all levels uncertain and fearful of their presence and activity in cyberspace. In addition, the economic and capitalist system in the Islamic Republic of Iran has always been the target of attacks by subversives and opponents, which can be seen in the form of cyber gambling networks, money laundering networks, illegal financial transactions, etc. Ultimately, what is most necessary, in addition to education, culture, supervision, infrastructure, control, etc., seems to be the creation of a coherent and efficient legal structure and the formation of a deterrent penal system that can make the user community prosperous by paying attention to the guidelines and creating obstacles to committing crimes in this regard.

SOURCES

[1] The Holy Quran
[2] Nahjul-Balagha
[3] Atkinson. R. F. (1989), An Introduction to the Philosophy of Ethics, translated by Sohrab Alavinia, Tehran, Center for Translation and Publishing of Books.
[4] Akhund Khorasani, Mohammad Kazem (1989), Kifayah al-Asul, Mehr Press, first edition.
[5] Amoli Mohammad Taqi (2005), Hayat Javid in the Science of Ethics, Mortazavi Publishing House, Editor: Akbar Safdari-Qazvini.
[6] Ansari, Najmeh and Arefkhani, Safar Ali (1982), Comparative Study of the Relationship between Jurisprudence and Ethics from the Perspective of Islam, Eighth International Conference on Religious Studies, Islamic Sciences, Jurisprudence and Law in Iran and the Islamic World, Tehran.
[7] Bahrami, Mohsen and Ah Faramarz Qaramaleki (2012), "Conceptual Analysis of Moral Conflicts", Ethics and Medical History, Fifth Volume, No. 2.
[8] Boazar Marcel (1989), Islam and the World of Today, translated by Masoud Mohammadi, Islamic Culture Publishing House.
[9] Khomeini, Seyyed Ruhollah (1999), Imam's Journal, Tehran, Institute for the Compilation and Publication of Imam Khomeini's Works.
[10] David Rene (1999), Great Contemporary Legal Systems, University Publishing Center, translated by Seyyed Izzatollah Iraqi, Mohammad Ashouri, Seyyed Hossein Safaei.
[11] Rouhani, Seyyed Mohammad (2004), History and Foundations of Political Thought in Islam, Reflection of Thought No. 49
[12] Shafi'i-Sarvostani Ibrahim (2016), Jurisprudence and Legislation: Pathology of Legislation in the Islamic Republic System, Taha Book Publishing.
[13] Sadr, Seyyed Mohammad Baqir (1979), Along with the Evolution of Ijtihad, translated by Ayatollah Seyyed Mohammad Baqir Sadr, Tehran: Roozbeh Publications.
[14] Tabatabaei, Mohammad Hossein (1981). Al-Mizan, translated by Mohammad Baqir Mousavi, Islamic Publications Office, Qom.
[15] Tusi, Jafar ibn Hassan (1986), Tahdhib al-Ahkam, research by Seyyed Hassan Mousavi, third volume, Tehran, Dar al-Kutb al-Islamiyyah.
[16] Alamzadeh Nouri, Mohammad; Hedayati Mohammad (2008), Comparative Comparison of Jurisprudence and Ethics, Pegah al-Hawza, No. 244
[17] Ghazali, Mohammad (2014), Revival of the Sciences of the Din, Vol. 2, Tehran: Ferdows Publications.
[18] Quarterly Journal of Jurisprudence (2004), Islamic Propaganda Office, taken from the article "Jurisprudence and Life", No. 39.
[19] Jurisprudence and Theory of Society Administration (1991), Hawza Magazine, No. 45.
[20] Feyz, Alireza (1992), Principles of Jurisprudence and Principles, Tehran, University of Tehran.
[21] Katouzian Naser (1991), Philosophy of Law, Volume 1, Ganj Danesh Publication, Third Edition.
[22] Majlesi, Mohammad Baqer (1985). Bihar al-Anwar, translated by Mousavi Hamedani, Tehran.
[23] Majlesi, Mohammad Baqer (1985). Bihar al-Anwar, translated by Mousavi Hamedani, Tehran.
[24] Motahari Morteza (2002), Riba, Bank and Insurance, Sadra Publishing House.
[25] Motahari Morteza (2002), Islam and the Needs of Time, Sadra Publishing House.
[26] Motahari Morteza (2003), Ten Words, Sadra Publishing House.
[27] Motahari, Morteza (2006), Introduction to Islamic Sciences, Vol. 3, Tehran: Sadra Publishing House.
[28] Mousavi Bojnourdi, Seyyed Mohammad (2014), The Role of Ethics in Jurisprudence and Law, out of place.