International Journal of Advanced Research in Humanities and Law (IJREL)
ISSN 2980-4043
DOI: 10.63053/ijrel.36

The Concept of Legislative Criminal Policy in The Blue of Cybercrimes

Mehrdad Falahi[1], Akbar Rajabi[2], Samira Golkhandan [3]

1. PhD student, Criminology, Azad University, Khomein Branch, Iran
2. Faculty member, Azad University, Khomein Unit, Iran (Corresponding Author)
3 .Faculty member of Azad University, Khomein, Iran

ARTICLE INFO

Keywords:
International Conventions on Cybercrimes - International Control - International Jurisdiction - Course of Disputes Due to Crimes - Criminal Deterrent Behavior

ABSTRACT

The emergence of the term criminal policy by Feuerbach, a German jurist at the end of the 18th century, was related to this rationalism in dealing with crime, and the word "policy" was born from it, which implies the concept of guided thinking and purposefulness, with a special meaning that is called Criminal "policy" has led to the acceptance and spread of this term in today's legal and sociological language, similar to the spread of terms such as "economic policy" and "cultural policy". One of the most important criminal policies of Iran in the prevention of computer crimes is its legislation in this field. Legislation in cyberspace can be explained with a three-step approach. Legislation in criminal law methods should start with recognizing the use of new technology and special departments along with police security structures or in the general concept of the police need to have the necessary conditions to investigate cybercrimes.

The third step is writing new rules. Based on experience, it may be difficult for legal authorities to implement the law-writing process for cybercrimes without international cooperation due to the rapid growth of network technology and its complex structures.

Introduction

Writing cybercrime laws separately may lead to conflicts of laws and waste of resources, and it is also necessary to follow the development of international strategies and standards. On the same basis, it can be said that the division of computer crimes on the one hand includes crimes against persons, against property, and crimes against public safety and comfort, and on the other hand, software crimes, data crimes, and crimes against individual privacy rights. Therefore, to prevent computer crimes, Iran's criminal policy in the legislative debate is to prevent potential and actual criminals from committing crimes by enacting laws in this area.

With the growth of new computer crimes in the current era, the police as one of the effective elements in the judicial policy of the country has taken measures to reform and transform its organizational structure according to this discussion, to create security in the production and exchange space. Information, along with the evolution of the security and law enforcement structure, means the formation of the production space police and information exchange based on the second strategy of the country's strategic document on the security of the production space and information exchange, which was approved by the Council of Ministers on 12/7/2007, a duty for the police force of the Islamic Republic of Iran. considered

If an international cybercrime occurs, many issues may arise regarding the criminal jurisdiction of this crime. The most effective way to solve this problem is to create a single principle for qualification in the field of global cybercrimes based on international laws. However, it still seems difficult to implement such a principle.

International cybercrimes happen regardless of place and time in international cyberspace. Under these circumstances, even if there is an international treaty on the criminalization of international cybercrimes, it would be useless if all the countries of the world do not participate in it.

In the event of a criminal act, as long as the criminal procedure is determined in a treaty, all the participating countries can have effective internal and external control over the crime based on a single principle. In contrast; When international cybercrimes are committed in cyberspace by criminals and the relevant country has not acceded to this treaty, that country does not necessarily need to coordinate with the criminal justice procedure defined by the treaty. As a result, internet crimes are borderless and we need uniform and universal laws and regulations to standardize the judicial procedures governing these crimes. International treaties based on voluntary national participation cannot guarantee the participation of all countries, therefore, it is very difficult to control Internet crimes in this way.

1- International convention on cybercrimes

1-1- Details and characteristics of the Budapest Treaty

The Budapest Convention is also known as the International Internet Crimes Convention and is the first international agreement created to deal with Internet crimes, which was signed by about 40 different countries at the Budapest International Conference on Internet Crimes on November 23, 2001, in Hungary. Since then, this treaty has been known as (Budapest Treaty). This agreement contains detailed definitions for all types of Internet crimes and the punishment for each is

specified.
In this agreement, computer systems, illegal access to information, violation of intellectual property law, production and distribution of computer viruses and promotion of child pornography are defined as criminal acts, and countries are obliged to join this law and prohibit such crimes in their domestic laws. He makes himself. All countries that have signed this agreement have the same laws and regulations to control Internet crimes and have provided a standard telephone line for this sector for international cooperation.

1-2-Achieved the Budapest Convention

1-2-1 Law Amendments In Cybercrimes

The achievement of this agreement is that it has made practical changes or rather a revolution in the legislation of Internet crimes. Around 2006, the Council of Europe launched a global project on cybercrime designed to strengthen internal stability based on the Budapest Treaty. The legal and institutional revolution regarding Internet crimes was recommended to about 120 different countries. Under the influence of this process, the United Nations General Assembly mentioned the Budapest Treaty as a basis for the development of laws and institutions for the investigation and prosecution of Internet crimes and proposed its accession to all countries of the world. The United Nations has played a pioneering role in standardizing the Budapest Treaty and managing its improvement (Jaejoon Jeong, 2013, 6 pp.125-127).

1-3 Formation of effective cooperation system for individual countries

Although the Budapest Treaty is an agreement made by the Council of Europe, today 55 countries have joined it. Considering that 14 European countries have not yet signed this treaty, this treaty has the potential to become a developed global treaty instead of a regional treaty in Europe.
Another advantage is that countries can prevent cybercrime by joining this treaty. In addition, its achievement will help the countries of the world widely in promoting general technologies on international cybercrimes.

1-4 Helping the public sector in increasing the ability to respond to cybercrimes

The legal and institutional revolution, as well as the effective cooperation of countries with each other, has led to the consolidation and accumulation of legal and institutional techniques in dealing with Internet crimes. Therefore, it seems that a positive impact should be given to it in terms of the prospect that they can help non-member countries, that is, to hold meetings together based on the Budapest Treaty. Having meetings like the one that led to Budapest acts like an accelerating catalyst for technological development in cybercrime management.
Also, this principle can be seen in Article 15 of the Budapest Treaty and it can be used as a manual to prevent internet crimes and use computers properly. Therefore, participation in this not only protects privacy but also personal rights.

1-5- Other achievements

The Budapest Treaty acts as a statute to increase the effectiveness of existing treaties in each country (in particular, the Treaty on Mutual Legal Cooperation, extradition for the execution of penalties in the treaty, etc.) judicial assistance for the investigation, arrest and trial of cybercrimes based on the Budapest Treaty, it increases the effect of other similar rituals.

1-6- International control of cyber crimes

1-6-1 Problems about the international criminal jurisdiction of cybercrimes

1-6-2 Solving the problem through current international laws

It is difficult for an international arbitration based on national participation to have a general obligation in reality, so it is better to resolve issues related to international cybercrimes through customary international law rather than treaties. When we talk about the establishment of customary international law, this does not require a universal similarity, but as soon as this law is created, it includes general binding factors. It is therefore reasonable to apply the same principles to international cybercrime laws through the requirements of customary international law.

7-1 Current law requirements in common international law

Current international laws are mainly based on national practices, but not all of them become a current laws. In the process of becoming a common law, "general practices" including continuity, uniformity, and generality must be considered. Also, the country in question must have legal approval in that section. The International Court of Justice (ICJ) has announced requirements for the establishment of current international law.

In this ruling, the International Court of Justice has concluded that the following conditions must be established for some of the provisions of the treaty as a common international law: 1- That article of law must have the characteristic of creating a norm 2- The participation of countries, especially countries whose interests are especially dependent on this practice 3- The functions of the country in question should be extensive and compatible 4- These practices should be considered as legal duties.

What needs attention here is the importance of "states whose interests are directly affected" for general measures to become common international law, they must be maintained for a certain period. However, there is no fixed period for the formation of its customs and practices. In this way, the current and general laws that have been created in countries have the possibility of becoming common laws, "extensive and compatible" in a short period.

8-1- Providing instructions through the United Nations and establishing conventional international laws

There should be consistent practices to establish common international law on criminal jurisdiction for international cybercrimes. In general, the meaning of method is uniform and continuous performance in countries. One of the most effective ways to form this practice is to create and publish a global guide reflecting the opinions of countries that have special interests in the field of international cybercrime, but there is still no valid binding legal system. It seems that such a code of practice should be developed by a global international organization that we call the United Nations. For the details of this Directive, it is reasonable for the countries affected to have jurisdictions consistent with the principle of territory and the principle of a passive person. The above guidelines have the possibility of being developed into common international law for the following reasons: 1- The principle of judicial unification for international cybercrimes is that it has a normative character 2- Countries affected by international cybercrime It is considered as one of those countries that have special interests and the participation of such countries is recommended. And if these procedures are to be formed, they must: 1- be widely followed. 2- be carried out under the legal certainty of the participating countries. As a result, this instruction will be registered as current international law.

1-9- Convention Problems In The Field Of International Cybercrimes

For the effective management of cyber wars that happened by a group of people against the construction of a nuclear power plant in Korea, the need for international cooperation to establish

cyber security with other countries, including the United States and China, has increased. On the same day, manpower and organization to control cyber terror in Korea should also be strengthened. Since December of last year, this group has continued its cyber psychological warfare (by disclosing information one after another), the first of which was information related to the nuclear energy information of the country of Korea, and then the Blue House of the National Intelligence Service and the Ministry of National Defense. targeted

The Korean government did not take any action except to establish a professional team such as the presidential security advisor team. A special adviser to the president is a non-permanent presidential official without experienced staff. Even the National Intelligence Service, which is responsible for cyber attacks, is itself suspected of being hacked.

While the BLUE HOUSE and the National Security Agency failed to properly control the cyber war, this hacker group continues to challenge and create cyber psychosis through the global Internet service, bringing it to the jurisdiction of Korea. Not covered What the relevant security company does is cooperate with the FBI by shutting down any website such as Twitter that contains such information, but this is also difficult without obtaining permission from Twitter.

Expanding the budget and strengthening the organization related to cyber security is an important and urgent issue. Last year, the President of the United States, Obama - after the Sony hacking incident - proposed the creation of an EGOV that would have public responsibility against cyber attacks. The department will be under the Office of Management and Budget (OBM) and will not only enforce cyber regulations but will also be tasked with overseeing and setting cyber strategy across various federal agencies. President Obama has submitted a 2016 budget proposal for the program in the amount of 130 million US dollars (about 120 billion Korean won) to Congress.

Last year, the Zionist regime also created a new department for national cyber security, which is called the "National Cyber Defense Organization". The National Cyber Protection Organization is a main centre for promoting cyber security policies in the medium and long term. The National Cyber Office, which is in charge of cyber security policies in national defence and government sectors and the security department, also covers all private sectors. This organization has created security jobs to strengthen the cyber protection system in cooperation with other organizations and companies and deals with crime, war, and terror in cyberspace. The international community works closely with this organization to investigate and control cyber threats. The FBI is investigating and working with 19 different countries to stop the effects of the world's largest online crime scene, Darkcode, and prosecute the hackers associated with it. Countries such as England, Australia, Canada, Bosnia, Croatia, the Zionist regime, and Romania are among these 19 countries.

During the secuInside meeting held in July, Blue House national security expert Jungin Lim emphasized that "due to the lack of sufficient international cooperation, Korea has difficulty in reviewing the output of nuclear power plant classes and nuclear energy. has been" and "to deal with Internet crimes" a global approach and preparation for international cooperation is needed (Helpless cybercrime, 2015.8.4)

Looking at the system of international cooperation regarding international cybercrime, we find that although treaties have been concluded and become effective, such as the Cyber Treaty of the Council of Europe (Budapest Treaty), the United Nations Convention against Transnational Organized Crime, the country of Korea He is not ready to join even a single treaty.

The most important reason for Korea not to join the international treaty is that according to the Budapest Treaty, what should be done before joining this treaty is that this country must establish a law for criminals and legal provisions for their punishment in Korea.

Of course, problems like this can be seen in the Korean constitution in professional sectors, which may be in front of the national law system or legal issues. Therefore, for such laws to be accepted, the sympathy of the nation must be aroused (Jeongil Jang, 2005. p. 350).

At this stage, the political community should discuss the problems and determine what needs to be revised in the law or the establishment of a new law in cooperation with the academic community in front of the national law. However, no effort has been made even by the government. Also, the opinions of the academic community indicate that Korea should actively explore the option of joining the international treaty, but the government only did the Cyberspace General Assembly on October 17, 2013.

Regardless of any type of international cooperation system, including the Budapest Treaty, which is growing despite the participation of most countries in the world and has been effective in controlling and eliminating Internet crimes, Korea should consider the details as soon as possible.

1–10- Cyber-attacks and crimes in international law

The transnational nature of cyber-attacks has caused the main concern of governments and countries to go beyond the national and sovereign level, and the international arena, which has faced many challenges in this field, has become the center of their attention, so the prevailing logic The international prevention of cyber-attacks should be formed with the international environment, different from the domestic space of the countries, while the borderless cyber space has created a virtual world parallel to the physical world, which in fact has legal control from The actions of a country are not made and naturally, the fight against crimes related to this field will also be outside the scope of the implementation of the domestic laws of the countries, in other words, the field of cyberspace law and the crimes committed in it are among the fields that due to globalization and its effects, It requires the adoption of uniform laws and regulations in the national and international space, therefore, in order to govern this space and make it legal, as well as to deal with the increasingly complex crimes committed in it, the cooperation and support of the international community is one of the basic and undeniable principles. It is in this context, in such a way that no criminal can remain unpunished by abusing the cross-border nature of the crimes committed under international codified laws.

In this regard, despite the various activities of international organizations to provide proposed regulations to unify and coordinate dealing with crimes in cyberspace, the world community is still in the early stages of achieving this goal and there are codified regulations that address the shortcomings of other regulations. It is necessary to resolve and be valid and have global acceptance.

Of course, the most logical option to create a unified and coordinated discourse with the aim of international prevention of cybercrimes is to explain solutions by the relevant international institutions, and at the head of them is the United Nations and its judicial pillar, the International Court of Justice, which according to the existing conditions, laws Explain the issue and consider the appropriate punishments for such crimes in the decisions and opinions.

In this regard, among the provisions of the United Nations Charter that can be used as a basis to fight against cybercrimes is Clause 4 of Article 2 of the United Nations Charter, which emphasizes that all members in their international relations should refrain from the threat of force or its use against territorial integrity. Or the political independence of any country or any other method that is based on the goal of the United Nations.

11–1- Examining cybercrime disputes in international law

The tremendous transformation and progress that we are witnessing today in the world of science

and technology; has such a speed that it continuously affects the important infrastructures of the society and creates major changes in it. Today it is called The technology that is the result of this development and progress called information technology, as it has brought us a new approach and a lovely space, as a result, the threats of this space are also worthy of consideration for individuals and society. The computer as a tool of information technology, due to its many capabilities such as high accuracy, high speed, large volume storage, information, tirelessness, fast exchange of information, easy access and countless other advantages, has brought many possibilities to mankind. But from another point of view, it has caused the emergence of new crimes that are not comparable to any of the existing classic crimes and may be more dangerous. The crimes of the new generation of information technology, whose platform computer and the global Internet network is one of its most important tools, are transnational crimes in the real sense and know no borders. Especially since crimes happen and often this environment exists in the space of the third generation of computers in the virtual environment of international networks in the world including the Internet and any interaction in data and information can promise the occurrence of a crime. Which in some cases are not compatible with classical and traditional crimes and in some ways are unprecedented and emerging crimes in any case, it is less possible to find the three elements of crime in terms of criminal law in such crimes and on the other hand international dimensions This type of crime has caused various people, including criminologists, lawyers, and computer experts, to study and comprehensively investigate this phenomenon; Because the formulation of laws and the implementation of punishments have become a complex issue due to the transnational nature of cybercrimes (Bastani, 2016). However, not many legal measures have been taken in the form and substance at the domestic and international levels by governments and institutions in the field of cybercrimes.

In the mid-1990s, a new generation of computer technology (which cybercrimes should be called the result of information and communication technology) appeared. In a very fast evolutionary process, computers became computer systems consisting of several computer devices that could communicate between systems and international networks. Computers have become more and more connected day by day through networks telecommunications and satellites, they have made it possible to receive, transmit, and issue signals, images, sounds, writings and symbols. Therefore, due to this great capability of communication technology, a huge transformation was created in the world of communication and the age of information technology. One of the characteristics of this new technology is the formation of communication between people of the nations of the world in a virtual space and the environment of international networks. In turn, it has a significant contribution in changing the form and function of social relations and, in the same way, it has created a transformation in changing the pattern of the nature of classic crimes (Zarger, 2015). The physical appearance of the criminal is at the place where the results of the crime occur, the time of the crime, the place of the crime, the victim and the form of the crime. To this type of crimes that occur in this (virtual) space; It is called cybercrime.

In cyberspace, the problems become more complicated to search and detect crimes. In the real world, a bank robbery is pretty obvious; Because after the robbery, there is no money in the bank's treasury. But in computer technology, the coffers can be emptied without any sign. For example, a thief can take a complete digital copy of the software and leave the original software as it was. In cyberspace, a copy is the same as the original. With a little work on the system, the thief can change the possibility of any investigation, such as erasing fingerprints. The most alarming aspect of cyberspace is the rapid spread of information in an instant. For example, in short moments, a part of the information that can potentially be misused is discovered (Bastani, 2013). Many hackers

(grey hat computer thieves) do not believe that what they are doing is wrong. They believe that hacking (stealing data or unauthorized access to the system) is just to satisfy their curiosity. Many hackers stay within the law, and even the minority of hackers who are involved in stealing computer systems and in their activities believe in the attitude of don't touch. Currently, it is not against the law in most countries to keep and share information about how to break into computer systems. However, using this information is against the law. But the danger arises when this information falls into the hands of evil people who have criminal goals. Cyber crimes have also become epidemic due to social and psychological reasons; Due to the virtual nature of cyberspace, some hackers see it as a game and have difficulty distinguishing cyberspace from the virtual world. For them, hacking is just an adventure they experience in the computer world. Unfortunately, these games have the same punishments and conditions as the real world. Unauthorized logging into the system for some teenagers has other social reasons. They hack sites that show their worth to those around them and gain value and respect. Hackers often exchange complementary methods among themselves.

A general definition describes cybercrime as any activity in which computers or networks are the means, target, or venue for criminal activity. The draft international convention refers to strengthening protection against cybercrime and terrorism. Cyber crimes are actions related to cyber systems. Some definitions try to take into account the goals and intentions and define cybercrimes more precisely. However, it should be noted that in the international and existing dimensions and the definition of crime in the legal perspective of the Islamic Republic of Iran, which acknowledges that: a crime is any act or omission for which a punishment has been determined in the law, so cybercrime can be implied It was defined as: Any action or omission that takes place in the cyberspace and is punished according to the law (Sobh Khiz, 2011).

1-12- Convention on cybercrimes

In 1997, "the Council of Europe, with the cooperation of 47 European countries, formed a committee of experts in the field of cybercrimes to identify and define new crimes, legal rights and criminal responsibility regarding the Internet" (Jalal Farahani, 2015: 22). Canada, Japan, South Africa and the United States were also invited to participate in this committee as observer countries. The goal was to create a set of standard laws on cybercrimes for the global community and to create a common criminal policy to prevent cybercrimes (Namayan, 2012:27).

The final result of the negotiations in the Committee of Experts led to the drafting of the Cybercrime Treaty in June 2010, which is currently the only global document in this field. "The treaty includes provisions in the fight against terrorism, sexual abuse of children, organized crime, copyright infringement and international cooperation between countries in the investigation and prosecution of cybercrimes. Although the parts of the treaty include a clear description of extradition" (Mirian, 1386:11).

The treaty gives police agencies expanded powers to investigate and prosecute computer crimes when these crimes cross national borders. On November 7, 2002, the Council adopted an additional protocol separate from the main cybercrimes, which organized racist computer material through computer networks.

After the Council of Europe finalized the treaty proposed by the 26 member states, it was signed in Budapest. Observer countries (United States, South Africa, Japan and Canada) had the option to sign it. It was then sent to other countries for approval. The treaty came into effect when five countries, including at least 3 member states of the Council of Europe, ratified it, and 23 countries signed it but did not ratify it. Although the approach of the treaty seems to be to fight cybercrime, it is clear that there are many symbolic elements in the treaty.

1–13- Treaty performance in moral education

Another symbolic policy evident in the Council of Europe's cybercrime treaty is ethical education. This treaty aims to help people learn what actions are correct and what behaviours are wrong about the Internet, and this education is because the Internet is a new phenomenon, some people are not sure which behaviour is right and which is wrong. These people need to be explained more about the acceptable and unacceptable behaviours related to the Internet.

The treaty also helps create "ethical agreement" both within a country and internationally about criminal behaviour on the Internet and provides definitions of crimes.

Although no punishments are specified in the cybercrime treaty, they are regulated by the specific rules of different countries. It serves to help citizens in terms of criminalization by reinforcing the idea that this behaviour is bad or wrong. These laws also provide assurance to those who do not commit cybercrime that they are acting appropriately and distinguish them from those who do. The treaty also provides public education about cybercrime and possible solutions.

1–14- Performance as an example and model for other countries

A third purpose of symbolic politics is to serve as a model for other governments. The Council of Europe Treaty fulfils this role. For those countries that do not have laws on cybercrime, this treaty serves as a model. The provisions of this treaty specifically specify which laws each state must adopt to be effective in combating cybercrime. Therefore, the Council of Europe seeks to model the laws that should be adopted that are more effective in dealing with the appropriate crimes, as a guide for any country that wants to develop laws to prevent Internet crimes" (Silver, 2001: 5).

The Cybercrime Act was passed by the United States Congress in 2002 as part of the Homeland Security Act. It provides tougher penalties for computer-related crimes. Offences that result in personal injury or death, such as life in prison.

In 2003, the UK passed a series of regulations forcing people to opt out of spam emails. It was called the Privacy and Electronic Communications Regulations. This law prohibited email without prior notice to the recipient. In the US in 2003, Congress passed the Unsolicited Pornography and Marketing Control, or Can-Spam Act, which went into effect in 2004. It requires senders to provide an optional option for receivers. (Kigerl.2009:573) Like the UK laws and regulations, this legislation imposed a series of criminal penalties and restrictions on the transmission of unsolicited e-mails, or many laws in many countries penalized the traditional and physical distribution of child pornography.

Therefore, the treaty forced the legislatures of the countries to re-examine and update their current laws. During the ratification process in the United States, it was decided that there were sufficient laws on treaty-compliant applications, forcing the Senate to review existing laws and determine whether they had been updated. or not

15–1- Performance As A Deterrent To Future Criminal Behaviour

The final element of a symbolic policy is that it serves as a deterrent to future criminal behaviour. The role of the treaty as a deterrent is questionable. The treaty did not specify a punishment for the crimes they specified, instead, each country was allowed to determine according to the structure and function of their crimes. This is what is perceived as a weakness in the treaty. (Coleman, 2003:136) Deterrents are then based on penalties and punishments set by individual governments rather than by an international organization. They were to refrain from committing cybercrimes because of the possibility of punishment.

In addition, since the treaty was not signed by all countries. It is clear that a significant number of countries have not implemented laws for cybercrime. For it to be a deterrent, more countries have

to sign the treaty and act on its mandate.

Conclusion

The exchange of information, the provision of evidence and the collection of evidence, the identification of the accused, the application of criminal jurisdiction, the pursuit of punishment and the extradition of their perpetrators, and finally the identification and execution of orders and criminal sentences are not provided in cybercrime cases. These types of crimes, due to their characteristics and coordinates, require such cooperation every day more than before. Cyberspace crimes are committed against the confidentiality and accessibility of computer systems or telecommunications networks. The services of such networks are used to commit traditional crimes. The cross-border nature of this type of crime conflicts with the territorial nature of the powers of the law enforcers. Therefore, different countries have concluded cooperation and negotiation that they have brought this area under the rule and Monitor those actions.

References

1. Hosseinikhah, Nouraleh (2018), Police and Computer Crimes, Tehran: Naja Ministry of Education and Training Publications.
2. Hosseinikhah, Nouraleh (2018), Police and Computer Crimes, Tehran: Naja Ministry of Education and Training Publications.
3. Zandi, Mohammad Reza (2014), preliminary research in cyber crimes, Jangal Publications
4. Aalipour, Hassan (2018), Information Technology Criminal Law (Computer Crimes), Khorsandi Publishing House
5. Aalipour, Hassan (2017), Information Technology Criminal Law, Second Edition, Khorsandi Publications.
6. Gregi, Marko, cybercrimes, a guide for developing countries, translated by Morteza Akbari, Najar, 2014.