International Journal of Culture and Modernity
ISSN 2697-2131, Volume 27 | Apr-2023
https://ijcm.academicjournal.io

55

Implementation of International Legislation in the Field of Information and Cyber Security in the Republic of Uzbekistan

Iminov Abdurasul Abdulatipovich
Alibekov Botir Sultanbekovich

ABSRACT

The article analyzes research data for the improvement of national legislation on the detection and prevention of offenses and crimes on the Internet. From this point of view, the author describes the need to consolidate at the international level the concept of offense and crime on the Internet, as well as to unify the legal norms in this area with the participation of all states, as well as to create a system of coordination and interaction of all existing services to counter this as within a separate state, and at the international level, employee training, international experience, implementation in legislation.

KEYWORDS: computer technologies, computer crimes, national legislation, computer fraud, computer sabotage, unauthorized access, interception of information, computer espionage, telecommunication networks, Internet, public safety.

In today's comprehensively developing world today, the number of users of cyberspace is dynamically growing, which is due to the general digital transformation of society, the high growth rate and demand for information and communication services. And this, in turn, sets the task of changing the legal policy of the Republic of Uzbekistan in the field of combating crimes in the field of digital technologies.

For effective counteraction to crimes in the field of digital technologies in the Republic of Uzbekistan with new threats emerging in the world, it is proposed to take new measures and improve state policy.

In the Republic of Uzbekistan, as of 2021, 100,015 domains of the national segment of the Internet ".uz" were registered, of which about 38,000 are active.

Of the 38,000 active domains, only 14,014 are secure, i.e. have an SSL security certificate. In other cases, either the certificate is expired - 613 cases, or is absent.

In 2021, the State Unitary Enterprise Cyber Security Center detected 17,097,478 cases of malicious and suspicious network activity originating from the address space of the national segment of the Internet. As part of the safe functioning of the websites of state bodies (round-the-clock monitoring of events and security incidents) for 2021, 636 events and incidents [1].

As of December 2021, 289 pornographic websites were identified in the national domain space and 91 more can serve the purposes of propaganda of immorality and moral corruption.

International Journal of Culture and Modernity
ISSN 2697-2131, Volume 27 | Apr-2023
https://ijcm.academicjournal.io

The above indicates the need to develop and adoption of a set of measures of legal, organizational and technical in nature to improve security in cyberspace.

Of particular importance for the improvement of national legislation are international legal documents that define the types of criminal acts, responsibility for them, and establish mechanisms for the implementation of international cooperation in this area.

European Committee on Crime Problems and a committee of experts on cybercrime developed the Convention on Computer Crime (Budapest, November 23, 2001) [2]. This document obliges the states that are its parties to harmonize national legislation regarding the definition of the main crimes specified in the document.

This document provides for the responsibility
for the following computer crimes:
– illegal access;
– illegal interception;
– impact on data;
– impact on the functioning of the system;
– illegal use of devices;
- forgery using computer technology;
- fraud using computer technology;
– offenses related to child pornography;
– copyright infringement offenses
and related rights.

In addition, on September 13, 1989, the Committee of Experts on Computer Crimes developed Recommendation No. R89 (9) of the Committee of Ministers of the member countries of the Council of Europe on crimes related to the use of a computer [3].

This Recommendation establishes crimes related to the use of computer technologies, and also gives a classification of computer crimes with the recommended and an optional list (minimum and additional lists) for inclusion in national legislation.

The "Minimum List of Offenses" includes:
1) computer fraud;
2) computer forgery;
3) damage to computer information or computer programs;
4) computer sabotage;
5) unauthorized access to the computer system;
6) unauthorized interception of information;
7) unauthorized use of protected computer programs;
8) illegal recreation of schemes.

"Additional list of offenses" includes the following four types of crimes:
1) illegal modification of computer information or computer programs;
2) computer espionage;
3) illegal use of a computer (without the appropriate permission);

International Journal of Culture and Modernity
ISSN 2697-2131, Volume 27 | Apr-2023
https://ijcm.academicjournal.io

4) unauthorized use of protected computer programs.

An analysis of the composition of these crimes in the above international acts shows that the list includes crimes in which computer information is the subject of an attack, as well as in which computer technologies are a way of committing, and through which they are committed.

The Criminal Code of the Republic of Uzbekistan provides for the following crimes related to the use of computer technology, information technology, telecommunications networks and the Internet [4]:

- Article 103. Driving to suicide (part 2, paragraph "d");
- Article 1031. Inducement to suicide (part 2, paragraph "c");
- Article 130. Manufacture, import, distribution, advertising, demonstration of pornographic products;
- Article 1301. Manufacture, import, distribution, advertising, demonstration of products that promote the cult of violence or cruelty;
- Article 139. Slander (Part 2);
– Article 1412. Violation of legislation on personal data;
- Article 167. Theft by appropriation or embezzlement (Part 4, Clause “d”);
- Article 168. Fraud (Part 2 p "c");
- Article 169. Theft (part 3, paragraph "b");
- Article 1881. Illegal activities to raise funds and (or) other property;
- Article 244. Mass riots (part 2, paragraph "b");
– Article 2441. Manufacture, storage, distribution or demonstration of materials containing a threat to public safety and public order (Part 3, Clause “d”);
- Article 2445. Dissemination of untrue information about the spread of quarantine and other infections dangerous to humans (part 2);
- Article 2446. Dissemination of false information;
- Article 278. Organization and conduct of gambling and other risk-based games (Part 3);
- Article 2781. Violation of the rules of informatization;
– article 2782. Illegal (unauthorized) access
to computer information;
- Article 2783. Manufacture for the purpose of sale or sale
and distribution of special tools to obtain illegal (unauthorized) access to a computer system, as well as to telecommunications networks;
- Article 2784. Modification of computer information;
- Article 2785. Computer sabotage;
- Article 2786. Creation, use or distribution of malicious programs;
- Article 2787. Illegal (unauthorized) access to the telecommunications network.

It should be noted that modern realities necessitate the introduction of additions and changes to the current legislation:

– in accordance with the adoption of the Law of the Republic of Uzbekistan

International Journal of Culture and Modernity
ISSN 2697-2131, Volume 27 | Apr-2023
https://ijcm.academicjournal.io

No. ZRU-764 “On Cyber Security” dated April 15, 2022, it is necessary to include an article in the Criminal Code providing for liability for a cyber attack on a critical information infrastructure object[5] ;

- in connection with the increasing cases in judicial practice, provide for liability in the Criminal Code and the Code on administrative responsibility for violating the rules of electronic commerce [6];

– analysis of foreign experience (Russian Federation, Republic of Kazakhstan, Republic of Moldova, Republic of Belarus, Republic of Azerbaijan, Republic of Georgia, Kyrgyz Republic) and law enforcement practice testifies on the need to combine Art. 2784 "Modification of computer information" and Art. 2785. "Computer Sabotage". Over the past 5 years, not a single crime has been registered under Art. 2785 "Computer sabotage." The differentiation of these two similar compositions causes difficulties for the law enforcement officer;

– to include the concept of digital evidence and a special procedure for their seizure in the Code of Criminal Procedure [7].

Comparative analysis of the norms of the international legal and national legislation on offenses and crimes in the information space shows hat most of the articles have already been implemented in the norms of national criminal legislation. National legislation covers international requirements and standards as much as possible. Accession of the Republic of Uzbekistan to these Conventions and Recommendations will expand the geography of circulation and access to information from state information databases, personal databases and other databases, at least in criminal cases on the territory of all states that have signed these international legal acts.

However, it must be taken into account that the adoption of these conventions and recommendations will impose on the Republic of Uzbekistan additional obligations provided for by these international acts.

The relevance of the fight against crimes on the Internet is due to the fact that their transnational nature requires concerted international efforts to combat them. In the conditions of constant improvement of methods and means of committing this kind of crimes, the importance of the activities of international organizations, and in particular Interpol, as a universal international organization that coordinates the cooperation of states in this area.

Back in January 2015, the members of the Shanghai Cooperation Organization submitted for consideration by the UN General Assembly the International Code of Conduct in the field of information security, which is the first international document dedicated to the norms of behavior in the information environment [8]. The document has the following purposes:

- define the rights and obligations of states in the information space;

– stimulate constructive and responsible behavior of the state;

– strengthen cooperation against threats and challenges in the information space.

International Journal of Culture and Modernity
ISSN 2697-2131, Volume 27 | Apr-2023
https://ijcm.academicjournal.io
59

In December 2018, the UN General Assembly adopted the resolution "Achievements in the field of informatization and telecommunications in the context of international security" [9], which was supported by

119 states, 46 countries voted against, 14 abstained. Since the code of conduct of States contained in the resolution on the Internet has a recommendatory character, work is underway on the development of the UN convention on international information security.

Socially dangerous acts in the field of information and communication technologies on the Internet, referred to as in the legal literature as cybercrimes, represent a global transnational threat to the world community. Unfortunately, it is impossible to solve this problem at the level of individual countries, for the reason that the specificity of this type of crime involves their commission in a different, virtual cyberspace, and in particular the Internet, which does not recognize the borders of states.

An urgent problem is to increase the effectiveness of the methodology for considering, disclosing and investigating offenses and crimes in the virtual space of the Internet. The main international coordinating, organizational structural unit that ensures efficiency in the field of international interaction, in the development of the best methodology for the law enforcement activities of national law enforcement agencies, is Interpol (International Criminal Police Organization (French Organization Internationale de Police Criminelle, OIPC, English International Criminal Police Organization, ICPO). The main task of Interpol is to unite the efforts of the national law enforcement agencies of the participating countries (194 states) in the field of combating common crime.

In each state-participant of this international organization of the criminal police, National Central Bureaus of Interpol (NCBs) are formed. Uzbekistan was no exception, where the necessary conditions for international cooperation in combating cybercrime have been created. Decree of the Cabinet of Ministers of June 2, 2017 343 approved a new version of the Regulations on the National Central Bureau of Interpol in the Republic of Uzbekistan[10], which supplemented the provisions on effective methods of investigating cybercrimes.

It should be emphasized that the National Central Bureaus (NCBs) are permanent law enforcement structural units of Interpol in a particular country and are endowed with broad powers to coordinate the fight with cybercrimes. It is they who represent the necessary intermediary bodies, which are the links of international cooperation of states in the fight against with cybercrime. The implementation of the coordinating mechanism is carried out through direct cooperation through the contacts of the NCB of the country and the General Secretariat of Interpol. A feature of the intermediary actions of the NCB is the fact that the instructions emanating from this international organization are of a recommendatory nature.

The NCB of Interpol in Uzbekistan is part of the structural unit of the Ministry of Internal Affairs on the rights of independent operational management, the main task of which is to ensure cooperation with law enforcement agencies of other Interpol member states in the disclosure and investigation of cybercrimes.

International Journal of Culture and Modernity
ISSN 2697-2131, Volume 27 | Apr-2023
https://ijcm.academicjournal.io
60

Interpol creates conditions for a uniform understanding and the use of a private forensic methodology for investigating crimes committed in the virtual space of the Internet. To do this, it is necessary to create a mechanism for the global harmonization of legal regulation of the fight against these types of offenses.

Based on the foregoing, it can be concluded that that the activities of Interpol in the coordination of international legal cooperation in the fight against crimes on the Internet are carried out in the following main areas:

1) in the international coordination of the activities of law enforcement agencies of individual states at the national level by developing uniform recommendations on the methodology for detecting and investigating offenses on the Internet;

2) in the creation of special coordinating units in the structure of Interpol, responsible for the implementation of optimal cooperation in the fight against this type of offense;

3) in the development and implementation of joint programs of practical activities to combat crime and crimes on the Internet;

4) in the development and adoption of the institutional framework for the activities of Interpol on the methods of combating these crimes;

5) in the adoption of the "Roadmap" for the implementation of the necessary measures for the exchange of experience and training of law enforcement officers of the participating States, as well as in the preparation of a methodology for the disclosure and investigation of offenses and crimes on the Internet.

International organizations such as the Organization for Economic Co-operation and Development, the Council of Europe, the European Union, the UN and Interpol play an important role in coordinating international efforts, building international cooperation in the fight against crime in the field of high technologies. Recognizing the danger of crimes in the field of information technology, their cross-border nature, the limited unilateral approach to solving this problem, it is necessary to study the developed international experience and develop proposals and recommendations for their implementation in national legislation.

From 1985 to 1989 The Special Committee of Experts of the Council of Europe on computer-related crime developed Recommendation No. 89, approved by the Committee of Ministers of the EU on September 13, 1989[11]. It contains a list of offenses recommended to the EU member states for the development of a common criminal strategy related to computer crimes. The document also noted the need to reach an international consensus on the criminalization of certain computer-related crimes. The recommendation contains two lists of crimes - "minimum" and "additional".

Based on the Budapest Convention, it is worth making proposals into national law.

Create lists of crimes indicating the acts themselves. For example, in the Budapest Convention, the “Minimum” list includes acts that must necessarily be prohibited by international law and subject to prosecution.

judicially. "Additional" list contains those offenses on which reaching international agreement is difficult.

International Journal of Culture and Modernity
ISSN 2697-2131, Volume 27 | Apr-2023
https://ijcm.academicjournal.io
61

1. Computer fraud. Entering, changing, erasing or damage to computer data or computer programs, or other interference with data processing that effects on the result of data processing in a way that causes economic or property loss to another person, committed with the intent to provide an illegal economic benefit for themselves or others.

2. Forgery of computer information. Entering, altering, destroying, concealing computer data or computer programs, or otherwise interfering with the processing of data in various ways, or causing such conditions that, under national law, would constitute such an offense as forgery in the traditional sense of this definition.

3. Damage to computer data or computer programs. Unauthorized destruction, damage, deterioration or suppression of computer data or computer programs.

4. Computer sabotage. Input, change, destruction or hiding computer data or computer programs or other interference with computer systems with the intent to interfere with the functioning of the computer or telecommunications systems.

5. Unauthorized access. Unauthorized access to a computer system or network in violation of security measures.

6. Unauthorized interception. Unauthorized interception of data going to the network, from the network or within the network, committed using technical means of communication.

7. Unauthorized reproduction of protected computer programs. Illegal reproduction, distribution or public transmission of a computer program protected by law.

8. Unauthorized reproduction of schemes. Unauthorized reproduction of circuit designs protected under the legislation on semiconductor products (programs), or commercial exploitation or illegal import for the purpose of commercial exploitation of a circuit or a semiconductor product as a product manufactured using these circuits.

Thus, in order to improve national legislation on the detection and prevention of offenses and crimes on the Internet, it is necessary first of all, the participation of all states, since these offenses are transnational in nature. It is necessary to consolidate at the international level the concept of offense and crime on the Internet, as well as to unify the legal norms in this area with the participation of all states. It is also necessary to create a system of coordination and interaction of all existing services to counter this, both within a single state and at the international level. Only through the implementation of law-making, institutional and organizational arrangements, including those listed above, and the participation of each state will make international cooperation in this area effective and successful.

LITERATURE:

1. In 2021, the State Unitary Enterprise Cyber Security Center detected 17,097,478 cases of malicious and suspicious network activity originating from the address space of the national segment of the Internet. As part of the safe functioning of the websites of state bodies (round-the-clock monitoring of events and security incidents) for 2021, 636 events and incidents.

International Journal of Culture and Modernity
ISSN 2697-2131, Volume 27 | Apr-2023
https://ijcm.academicjournal.io
62

2. European Crime Committee and a committee of experts on cybercrime developed the Convention on Computer Crime (Budapest, November 23, 2001).
3. On September 13, 1989, the Committee of Experts on Computer Crimes developed Recommendation No. R89(9) of the Committee of Ministers of the member countries of the Council of Europe on computer-related crimes.
4. The Criminal Code of the Republic of Uzbekistan (approved by the Law of the Republic of Uzbekistan dated September 22, 1994 No. 2012-XII) (as amended and supplemented as of 10/19/2022
5. Law of the Republic of Uzbekistan No. ZRU-764 "On Cyber Security" dated April 15, 2022, it is necessary to include an article in the Criminal Code providing for liability for a cyber attack on a critical information infrastructure[5]
6. Code of the Republic of Uzbekistan on administrative responsibility (approved by the Law of the Republic of Uzbekistan dated September 22, 1994 No. 2015-XII) (as amended and supplemented as of December 16, 2022)
7. 01.04.1995 CRIMINAL PROCEDURE CODE OF THE REPUBLIC OF UZBEKISTAN
8. In January 2015, the participants of the Shanghai Cooperation Organization submitted for consideration by the UN General Assembly the International Code of Conduct in the field of information security, which is the first international document dedicated to the norms of conduct in the information environment [8].
9. In December 2018, the UNGA adopted a resolution "Achievements in the field of informatization and telecommunications in the context of international security" [9],
10. Decree of the Cabinet of Ministers of June 2, 2017 No. 343 approved a new version of the Regulations on the National Central Bureau of Interpol in the Republic of Uzbekistan[10],
11. Recommendation No. 89 approved by the EU Committee of Ministers on 13 September 1989[11].