CZU: 343.346.8(479.24):343.85 **DOI: 10.5281/zenodo.7358911**

INTERNATIONAL ACTIONS IN THE FIELD OF CYBERCRIME IN MODERN TIMES AND THEIR EFFECTS ON AZERBAIJAN LAW SYSTEM. LEGISLATION AND PRACTICE OF INDIVIDUAL STATES IN COMBATING CYBERCRIME

MUSAYEV Erkin,

full-time phd student,Baku State University, Faculty of Law
ORCID: 0000-0003-4428-0668

Devenind cel mai grav flagel al actualei „epoci a calculatoarelor”, infracțiunile informatice s-au extins în întreaga țară, dobândind noi forme. În prezent, ținând cont că infracțiunile informatice sunt larg răspândite și se dezvoltă rapid, combaterea acestora a devenit una dintre sarcinile principale ale Republicii Azerbaidjan în contextul luptei împotriva criminalității. Cu toate acestea, o serie de probleme legate de investigarea criminalității informatice, inclusiv implementarea măsurilor preventive, fac dificilă identificarea acestora. Problema principală este caracterul anonim al infracțiunilor informatice. Această caracteristică se atribuie doar infracțiunilor informatice, care reprezintă o problemă a criminalității prin internet, deoarece există atât de multe modalități de a masca identitatea. Această caracteristică face imposibilă investigarea infracțiunilor cibernetice, în special a celor desfășurate pe internet. Acest aspect face mai dificilă identificarea infractorilor. În cele din urmă, trebuie menționat faptul că infracțiunile informatice au început să se extindă sub aspect geografic în ultimii ani. Infractorii cibernetici pot deja accesa cu ușurință conturi bancare din alte țări, sisteme informatice guvernamentale și pot efectua tranzacții asociate pe teritoriul unui stat. În acest context, cooperarea internațională în lupta împotriva criminalității informatice, semnarea acordurilor bilaterale și multilaterale cu alte țări, precum și dezvoltarea unor metode și tehnici comune de combatere a acestor infracțiuni va facilita lupta împotriva acestor infracțiuni și va genera rezultate pozitive.

Key words: *cyber crime, information technology, computer system, information security*

International agreements to which the Republic of Azerbaijan is a party constitute an inherent element of Azerbaijan's legislative system, according to the Constitution of the Republic of Azerbaijan.

According to Article 151 of the Azerbaijan Republic's Constitution, in the event of a dispute between the Republic of Azerbaijan's normative legal actions (except the Republic of Azerbaijan's Constitution and those established by referendum) and the interstate agreements to which the Republic of Azerbaijan is a party, the international accords should be enforced. [1]

The Republic of Azerbaijan's criminal law is founded on the basis of legality. The contents of the "Universal Declaration of the Rights of Belief" are closely related to the instruction of paragraph 8 of Article 71 of the Constitution of the Azerbaijan Republic. "No one can be held liable for an act that was not

regarded illegal at the time it was committed," declares Article 71, paragraph 8. The stance of this article is likewise confirmed by Article 3 of the Criminal Code.[2]

Although the Republic of Azerbaijan's criminal law is founded on the basis of legality and does not accept similarities, it is critical to identify the Azerbaijani government's international policy in the fight against cybercrime and to further develop cybercrime combat tactics.

It is impossible to discuss cybercrime without mentioning the European Convention, to which the Republic of Azerbaijan is a signatory.

Infringement of information content violations are addressed in Chapter 3 of the Covenant. The Convention covers a number of substantive and procedural laws, as well as a number of material crimes (child pornography distribution, copyright and related rights violations) and procedural aspects (legal persons subject to these crimes, scope of procedural norms) that are not covered by the Azerbaijani Criminal Code.

In addition to the offences outlined in the sphere of cybercrime, the European Convention, to which the Republic of Azerbaijan is a party, contains a number of other criminal acts. The following are examples of such elements:Counterfeiting using computer technology; Fraud using computer technology, Offenses related to child pornography, Offenses related to copyright and related rights.

The contract's objective and the parties' obligations are represented in the Preamble. According to the Preamble, member states agree to cooperate in this area, including through legislative changes.

The benefits of this deal in the battle against cybercrime for the Republic of Azerbaijan are undeniable. As a result of the Convention's acceptance, some revisions to the Criminal Code in the area of cybercrime were made.

This Agreement considers copyright infringement, which is still important in today's world, to be a criminal act. Member States' obligations under the Paris Law of July 24, 1971, amending the Berne Convention for the Protection of Literary and Artistic Works, the Agreement on Commercial Aspects of Intellectual Property Rights, and the World Intellectual Property Organization Copyright Convention are being carried out.

In addition, the Convention reflects procedural issues related to crimes in this area, including additional types of liability and sanctions, jurisdiction, general principles and a number of other specific provisions.

In addition, the Republic of Azerbaijan adopted a number of Declarations arising from the Convention. These include:

In line with article 24, paragraph 7, subparagraph (a) of the Convention, the Republic of Azerbaijan appoints the Ministry of Justice as the competent authority to consider petitions for extradition and interim detention in the absence of an extradition treaty.

1. In accordance with subparagraph (c) of paragraph 2 of Article 27 of the Convention, the Republic of Azerbaijan appoints the Ministry of National Security as the competent authority responsible for the sending, execution, and execution of requests for mutual assistance.

2. The Secretary General of the Azerbaijan Republic proclaims that investigations under this paragraph should be sent to the central authority for effectiveness, in accordance with subparagraph (e) of paragraph 9 of article 27 of the Convention.

3. The Republic of Azerbaijan, in accordance with Article 35, paragraph 1 of the Convention, may appoint the Ministry of National Security as a coordinating body, working twenty-four hours a day, seven days a week, to provide emergency assistance in the collection of electronic evidence for the purpose of investigating or otherwise prosecuting crimes involving computer systems and data.

4. In line with Article 38 of the Convention, the Republic of Azerbaijan declares that it cannot ensure the implementation of the Convention's provisions in the territories occupied by the Azerbaijan Republic until the lands are liberated.

5. In connection to subparagraph (b) of paragraph 1 of article 6 of the Convention, the Republic of Azerbaijan announces that activities that are not considered imminent danger due to their insignificance are considered a penal offence, not a crime. If committing a socially risky behavior (action or omission) that is prohibited under the prospect of penalty causes serious harm, it is a crime.

6. Unless the actions of the Republic of Azerbaijan referred to in Article 6 (1) of the Convention in accordance with Article 6 (3) of the Convention are considered a socially dangerous crime because of their insignificance, accepts it as punishable, not a criminal offence, and states that criminal liability will only arise if the acts in question cause significant harm.

7. Criminal culpability arises only if the conduct referred to in article 4 of

the Convention cause severe harm, according to the Republic of Azerbaijan's interpretation of article 42 and paragraph 2 of article 4 of the Convention.

8. The Republic of Azerbaijan, in accordance with article 42 and article 29, paragraph 4 of the Convention, when a crime on which the data protection request is based, it has the right to refuse to fulfill the data protection request, unless the crime is considered a crime according to the legislation of the Azerbaijan Republic.

Because it was the Ministry of National Security at the time, the authorities in this sector were transferred to that institution, as can be seen from the explanations. The State Security Service currently has the listed powers.

Furthermore, our country's initial statement concerns the question of return. Extradition, or the transfer of a person to another country, is governed under Article 13 of the Criminal Code. In addition, the subject of cyber offenders' extradition is handled in accordance with the statement.

It should also be noted that, R (85) 10, Common opinion on the practical application of the section of the Committee of Ministers of the European Convention on Mutual Legal Assistance in Criminal Matters on court orders to intercept telecommunications information in accordance with the obligation arising from the above-mentioned reasoning; R (88) 2 on the fight against piracy in the field of copyright and related rights; R (87) 15 on police use of personal data; telecommunications services, R (95) 4 on the protection of personal data, particularly in the field of telephone services; as well as defining the concepts of some computer crimes should take into account Recommendation R (89) 9 on computer crime and R (95) 13 on information technology issues of criminal procedure law, which provides guidance for national legislatures.

Let's take a look at some of the suggestions in this Advice.

The state is responsible for copyright protection, according to Recommendation 88. As we all know, the Internet is the primary conduit for copyright infringement, which links these infractions to cybercrime. As a result, authorities must ensure that the rights of writers, artists, producers, and publishers are appropriately protected in the battle against cybercrime.[3]

States must comply with Recommendation R (95) 4 on the protection of personal data in the sphere of telecommunications services, particularly telephone services. According to this judgement, the government may only interfere with natural or legal people' telephone calls and other kinds of

communication when required by law and when necessary for a democratic society:

1. to protect relevant information or the rights and freedoms of others;
2. to defend state security, public safety, the state's monetary interests, or the prevention of other crimes.

It is apparent that the state's rights have been strengthened in this area in order to combat cybercrime. This circumstance makes it easier for the government to detect criminal activity in this area.

(89) Recommendation 9 lays out principles for national legislatures to use in defining the terms "particular computer offenses."

In addition, it is more appropriate to examine the above-mentioned decision together with the Council of Europe's Recommendation R (95) 13 on criminal procedure law issues related to information technologies and to conduct an investigation within the scope of the following criminal acts:

1. cybercrime, especially those conducted through the use of telecommunications networks, such as the Internet, for example, unlawful money transactions;
2. in the sphere of cyberspace, definitions, penalties, and obligations of organizations, as well as substantive criminal law difficulties in other domains;
3. Taking into account the issues that encryption, access codes, and other unique information security measures might cause;
4. Forensic concerns relating to computer crimes, such as locating the crime (locus delicti) and determining which law applies. As a result, in most circumstances, the problem that is not bis idem should also contain the topic of how to settle authority disputes and positive authority conflicts, as well as how to avoid negative authority conflicts;
5. problems of international collaboration in cybercrime investigations;
6. international cooperation in cybercrime investigations.

The Republic of Azerbaijan's efforts for international collaboration in the fight against cybercrime present themselves in a variety of ways, in addition to international measures.

On October 6, 2011, the OSCE Office in Baku hosted an international conference aimed at identifying and expanding measures to combat cybercrime. One of the most important problems raised was the expansion of international collaboration in this sector.

It is beneficial to examine international laws of other countries in order to

have a thorough understanding of the Republic of Azerbaijan's cybercrime policy, as well as the efficiency of the measures and procedures employed.

It's worth noting that the French Criminal Code (1992) included a separate section on "attempts against the automated data processing system" to address cybercrime for the first time in history.

Because the nature and dynamics of crime change by country, and crime is tied to time and geography, various countries have varied methods and protective systems when it comes to cybercrime. Let's have a look at the differences in three different scenarios.

The Republic of Turkey.

When we look at the legal legislation of the Republic of Turkey, we can notice that the Turkish Penal Code has a specific section on cyber offences.

243-246 of the Turkish Penal Code, Chapter 10. These offences are governed by articles.[4, p. 66]

Access to the information system is covered under Article 243. A person who joins or remains in an information system partially or entirely illegally and stays there is penalized with up to one year in prison or a judicial fine, according to the article's order. As a result of this conduct, destroying or modifying the information in the system is classified as an aggravating circumstance, with penalties ranging from six months to two years in jail.[4, p. 66]

"Blocking, damaging, deleting, or modifying the system" is the title of Article 244.[4, p.66]

(1) Anyone who interferes with or disrupts the operation of an information system faces a sentence of one to five years in jail.

(2) Anyone who breaches, destroys, modifies, or renders inaccessible information in an information system, places information in the system, or sends existing information to another location faces a six-month to three-year jail sentence.

(3) The punishment is doubled if these crimes are committed on a bank or credit institution's information system, including a public institution or institution.

(4) The conduct of an act listed in the preceding subsections is punishable by imprisonment for two to six years or a fine, unless the person's unfair gain for his or another's advantage produces a different punishment.

Article 245.– Fraudulent use of a bank or credit card[4, p. 66]

(1) A person who seizes or keeps, uses or gives to someone else a bank or credit card belonging to another person in any way without the consent of the card holder or the person to whom the card is to be issued, in cases where benefit is provided to himself or to someone else in this case that person punishes with imprisonment from three to six years and a court fine of up to five thousand days.

(2) Producing, selling, delivering, buying, or accepting fraudulent bank or credit cards in connection with other people's bank accounts is punishable by three to seven years in jail and a court punishment of up to ten thousand days.

(3) A person who gives herself or another person with a benefit with the intent of using a phony or fake bank or credit card is sentenced to four to eight years in jail or a fine, unless the conduct results in another offense requiring a harsher penalty.

(4) In the first paragraph,

a) One of the people against whom a divorce decree has not been issued,

b) a descendant or parent, or one of their close relatives, or an adoptive or adoptive parent, or a descendant or parent, or one of their close relatives, or an adopted or adoptive parent,

c) One of the brothers living in the same place,

In case of damage, close relatives will not be punished.

Article 246.– (1)Special security measures are applied to Legal persons who are given unfair advantage due to the crimes specified in this article.[4, p. 67]

In addition, the Istanbul Cyber Crimes Branch (Istanbul Cyber Crimes Branch) works in Turkey to combat cybercrime.

United States of America.

The United States is the country most afflicted by cybercrime, according to data. According to a study conducted by the US Federal Bureau of Investigation in early 2004, 90% of the Fortune 500 corporations examined reported security breaches, with 80% of them suffering financial losses.[5, p 98] To combat internet crime, the Federal Bureau of Investigation has set up an online employer registration program.

In this sense, US law prioritizes the fight against cybercrime and provides extensive coverage in its legislation. In this category, the US Penal Code includes the following criminal elements:[6]

18 USC. § 1028 - Identity card, identity fraud and related activity features and information

18 USC. § 1028A - Theft of personal data

18 USC. § 1029 - Fraud and related activities related to access devices

18 USC. § 1030 - Computer fraud and related actions

18 USC. § 1037 - Email fraud and related actions

18 USC. § 1343 - Fraud on the telephone, radio, and television

18 USC. § 1362 - Fraud involving communication lines, stations or systems

18 USC. § 1462 – Pornographic videos can be imported or moved.

18 USC. § 1465 - Pornographic products are transported for the purpose of sale or distribution.

18 USC. § 1466A - Visually stunning depiction of child sexual abuse.

18 USC. § 2251 - children's sexual exploitation

18 USC. § 2252 - Minors are sexually exploited in activities using specific narcotics.

18 USC. § 2252A - Certain activities with a substance that is or contains child pornography are prohibited.

18 USC. § 2252B - On the internet, do not alter(change) domain names.

18 USC. § 2252C - İnternetdə yanlış sözlər və ya rəqəmsal şəkillərdən istifadə etmə

18 USC. § 2425 - Interstate facilities are being used to send information on a youngster.

18 USC. § 2319 - copyright infringement

17 USC. § 506 – Other infringements of copyright

47 USC. 605 - Use of unlicensed transmission or communication

18 USC. §§ 2510-2522 - Telephone, verbal, or technological communication is disrupted.

18 USC. §§ 2701-2712 - Recorded telephone and electronic communications: protection and disclosure

18 USC. §§ 3121-3127 - Pen and paper notes, as well as capturing and tracking gadgets

The United States' Information Technology Act of 2000 has proven to be one of the most successful instruments in the battle against cybercrime. This law made it possible for anyone to send money using entirely safe and secure credit cards. All papers are required by law to be digitized.

Russian Federation

The Russian Federation's Criminal Code features a specific section on cybercrime.

Chapter 28. Computer data crimes

Article 272. Unauthorized access to computer data[7, p.135]

1. Unauthorized access, deletion, blocking or copying of computer data protected by law relating to electronic computers, their systems and networks or their carriers, two hundred thousand five hundred minimum wage, convict salary or other income between two and five months that disrupts the functioning of electronic computers, systems and networks, Refineries operate for six months to a year or jail terms of up to two years.

2. The same acts committed with the prior consent of a group of persons or by an organized group or by abuse of official duties are punishable by a fine of at least five hundred manats to eight hundred manats, Refineries may be sentenced to imprisonment from one year to two years, from three to six months or to imprisonment for up to five years.

Article 273: Dangerous electronic computer programs: creation, use, and distribution[7, p.136]

1. Production of electronic computer programs or changes to existing programs, deleting, blocking, changing, or copying information that disrupts the operation of electronic computers, systems, or networks and causes these programs to be used or distributed, at least two workers 500, for a period of two to five months shall be punished with a fine of up to three years, plus salary or other income.

2. A similar crime with significant effects carries a sentence of three to seven years in jail.

Article 274. Violation of an electronic computer's, system's, or network's operating regulations[7, p 137]

1. A person who has access to electronic computers, systems, or networks, in particular if a violation of the operating rules of an electronic computer, system, or network results in the deletion, blocking, or alteration of information in violation of the law, resulting in imprisonment for up to five years and serious harm, from 180 to 200 hours of forced labor or up to two years of freedom restriction.

2. A similar crime with significant effects is penalized by up to four years in jail.

According to the information shown above, the structure and dynamics of cybercrime vary by nation. However, there are major general tendencies in the growth of crime for different countries throughout the world, in addition to the aforementioned.

References:

1. The Constitution of the Republic of Azerbaijan: http://www.e-qanun.az/framework/897
2. The Criminal Code of the Republic of Azerbaijan: http://e-qanun.az/framework/46947
3. Recommendation No. 2 R (88) on combating piracy in the field of copyright and related rights
4. The Turkish Penal Code: https://www.mevzuat.gov.tr/mevzuatmetin/1.5.5237.pdf
5. Moore, R. (2005) “Cyber crime: Investigating High-Technology Computer Crime”, Cleveland, Mississippi:Anderson Publishing.
6. U.S. Code: Title 18- Crimes and Criminal Procedure OLRC: https://uscode.house.gov/browse/prelim@title18&edition=prelim
7. The Criminal Code of The Russion Federation: https://www.legislationline.org/download/id/4247/file/RF_CC_1996_am03.2012_en.pdf