Musayev E.H.♦

DOI: 10.25108/2304-1730-1749.iolr.2023.70.97-100
UDC: 343.98

Cybercrime's Subjective Manifestations

Abstract: As in any field, there are disadvantages to the development of technology. In the last decades of the twentieth century, as a result of the progressive development of technology, significant changes have been observed in the state and dynamics of crime worldwide. Thus, new crimes have emerged and expanded in the digital and virtual spheres, creating legal threats to people's lives.

These violations, defined as crimes, are in theory "computer crimes", "computer-related crimes", "electronic crimes", "digital crimes", "high-tech crimes", "information crimes", "cybercrime" and so on is called.

For this reason, in the article, the criminal composition of cybercrimes was investigated in more detail and the subjective and subjective aspects of acts considered cybercrime according to the Criminal Code of the Republic of Azerbaijan as a socially dangerous act were studied.

Keywords: cybercrime; computer system; computer data; digital information.

It's crucial to understand the nature of cybercrime by identifying its subjective qualities, such as the topic matter.

The mental activity of the individual directly involved in the conduct of the crime is the subjective part of the crime. The subjective component is a "model" of the objective aspect that has been transmitted to the subject's soul. Distinct crimes may have different "subjects" and "forms" when it comes to the subjective component.

The subjective part of crime is a mental attitude toward a socially harmful behavior in the form of conspiracy and neglect. The urge to conduct a socially risky activity, the mental understanding of the action's objective elements, and the attitude toward it are all expressed in the subjective part of crime [2, p. 193]. The storyline can be both direct and indirect, depending on the facts of the repercussions.

The subjective part of the crime, according to Naumov, is a feature of the internal content of the crime (as opposed to the objective side); it consists of the subject's guilt coupled with a unique mental attitude toward the unlawful conduct and its repercussions. Intent or omission, as well as motive and goal, are all factors to consider.

The following are the aspects of the subjective side of the crime:

- *Guilt (Conspiracy And Negligence)*
- *Motive*
- *Aim*
- *Applies To Emotional State.*

♦ **Musayev Erkin Humbat oglu** - Full-time PhD student in Criminal Law and criminology; Criminal-enforcement law at the Criminal Law and Criminology Department of Faculty of Law of Baku State University (Azerbaijan). E-mail: musayev2022@gmail.com

All parts of the crime include the characteristics that distinguish intent or carelessness from the subjective portion of the crime. As a result, the culpability in determining criminal liability should be explained in some way.

It also has aspects like the subjective aspect, motive, and goal. The motivation for crime is the desire to conduct a socially risky behavior based on a perceived interest in that act. The person's idea of the intended change that the crime to be committed would bring about in the outer world is the motive of the crime [2, p.226].

A person who has performed a socially harmful conduct and is capable of criminal culpability is the subject of the crime.

Cybercrime is committed with deliberate purpose and is subjective. The intentions and goals of such acts are crucial in revealing their subjective nature.

A sane individual above the age of 16 is the target of cybercrime.

The offense of unauthorised access to a computer system is subjectively committed with direct purpose, according to Article 271 of the Penal Code.

The idea of approaching with a new goal in mind is extremely intriguing. Access to a computer system for other objectives, according to the authors, might take the form of deleting information about a person or another person, shutting down the system, installing harmful software, or unfair competition.

It's possible that the goal here is to seize computer data or something else entirely. The major motivation is the desire to conduct a socially harmful activity based on a perceived interest in a certain action.

The person's view of the intended change that the crime to be committed would cause in the outer world is the goal of this crime.

Computer data can be saved in any location on the computer. Various sorts of discs, conductors, and magnetic-optical discs are examples of these storage components (CD, DVD, etc.).

It is handled subjectively with direct purpose. A person who accesses a computer system knows he has no permission to be there, that he is violating security procedures, and that he wants to be there. This article also covers the collection of information without breaking security measures and the gathering of information for other personal reasons [3, p. 453].

The subject of the mentioned offense is someone who does not have the authority to access the computer system or any component of it. Persons whose professional activities are continuously or temporarily associated with the supply of a computer system, or any component thereof, for legal reasons may use this privilege.

Persons who are not directly linked to computer information or hardware devices, but who have access to the locations of computers, systems, or networks, but do not have the authority to access a computer system or any portion of it, are susceptible to the violation outlined in this article.

At the same time, the Criminal Code's Article 99-4. A legal person might likewise be the victim of this crime, according to the article.

Illegal computer information seizure is a felony performed with subjectively direct intent. In this scenario, the person is aware of the public threat of intercepting computer data that is not intended for lawful use, including electromagnetic radiation from computer systems carrying such data, without the right to utilize technological methods, and intends to seize it.

The subject might be a responsible person above the age of sixteen. A person who is the carrier of computer data is not authorized to receive electromagnetic radiation from computer

systems, which is the subject of the crime. Persons whose professional activities are continuously or temporarily involved with the normal running of a company may have such a privilege.

Persons whose professional activities are continuously or temporarily linked to the regular operation of a computer system or network may have such a privilege.

Articles 99-4 of the Criminal Code, in particular. Legal entities, according to the article, can be held liable for the offense.

A sane 16-year-old person, including a legal person, may be the subject of the offenses described in paragraphs 1 and 2 of Article 273 of the Criminal Code.

According to article 273.1, this offense is committed by sane people who do not have the right to deal with computer data and do not have the right to delete, edit, or modify it.

Here, the mental attitude of the perpetrator to his actions is in the form of a direct conspiracy of guilt, and there is a direct or indirect conspiracy regarding the fact that socially dangerous consequences occur with significant harm.

The subject of article 273.2 is also special, ie a person who does not have the right to work in a computer system, enter information into a computer, transfer data, etc.

It understands the public danger that the methods listed in paragraph 2 of this article will seriously interfere with the operation of the computer system and wishes to create such an obstacle. The motive here is not the main feature of the crime.

The offence is committed with direct purpose, according to article 273-1.1 of the Criminal Code. It produces, imports, maintains, installs, distributes, and facilitates the acquisition of equipment and computer programs, knowing that a person is prepared and adapted to perform a cybercrime, and wants that these activities do serious harm.

Committing a cybercrime is the goal of committing a crime. Despite the fact that this is listed as a goal in the article's structure, it should be considered as the crime's cause. Cybercrime cannot be defined as a goal; it can only be defined as a person's purpose [1, p. 885].

Article 273-1 - Access to computer data stored in a computer system or any part of it for the purpose of seizing it, article 271 of the Penal Code imposes liability regardless of whether such information is of personal, public or government importance and whether it is obtained as a result of access to the information.

Paragraphs 2 and 3 of this article are also subjectively committed with direct intent and with the intent to commit a cybercrime for a specific purpose.

A sane person above the age of 16 who does not have the right to input information or operate with a computer, according to Article 273-2, might be the subject of the infraction.

Subjectively committed with the express intent and for a specific goal - to create or utilize false computer data as actual data. The individual anticipates and desires to avert a public hazard, such as the introduction of fake computer data into a computer system, the replacement of actual data with fake data, the deletion or blockage of data, and therefore the violation of the original computer data's authenticity [4, p. 137].

References

1. Commentary to the Criminal Code of the Republic of Azerbaijan: edited by F.Y. Samandarov. Baku, Digesta Publ., 2007, 959 p. (in Azerbaijani).

2. Samandarov F.Y. Criminal Law (General Part) Textbook. Baku, Legal Literature Publ., 2002, 736 p. (in Azerbaijani).

3. Cybercrime and Digital Forensics: An Introduction (3rd Edition), (Thomas J.Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar), Routledge Publisher, 2022

4. Cyberspace, Cybersecurity, and Cybercrime, (1st Edition),(Janine Kremling, Amanda M. Sharp Parker), SAGE Publications Inc, 2017.

Мусаев Э.Г.♦

DOI: 10.25108/2304-1730-1749.iolr.2023.70.97-100
УДК: 343.98

Субъективные признаки киберпреступлений

Аннотация: Как и в любой сфере здесь тоже имеются свои недостатки. В последние десятилетия XX века в результате опережающего развития технологии в мире наблюдаются существенные изменения в динамике преступности. Таким образом, появились новые преступления в цифровой и виртуальной сфере, создавая юридические угрозы в жизни людей.

Эти нарушения в теории квалифицируются как «компьютерные преступления», «преступления связанные с компьютером», «электронные преступления», «цифровые преступления», «высокие технологические преступления», «информационные преступления», «киберпреступления» и т.д.

По этой причине в статье более подробно исследован преступный состав киберпреступлений и изучены субъективная и субъективная стороны деяний, считающихся киберпреступлениями согласно Уголовному кодексу Азербайджанской Республики общественно опасными деяниями.

Ключевые слова: киберпреступность; компьютерная система; компьютерные данные; цифровая информация.

Библиография

1. Комментарий к Уголовному кодексу Азербайджанской Республики. Под ред. Ф.Ю.Самандарова. – Баку: Дигеста, 2007. – 959 с. (на азерб. яз.).

2. Самандаров Ф.Ю. Уголовное право (общая часть) Учебник. – Баку: Изд-во Юридическая литература, 2002. – 736 с. (на азерб. яз.).

3. Cybercrime and Digital Forensics: An Introduction (3rd Edition), (Thomas J.Holt, Adam M. Bossler, Kathryn C. Seigfried-Spellar), Routledge Publisher, 2022

4. Cyberspace, Cybersecurity, and Cybercrime, (1st Edition), (Janine Kremling, Amanda M. Sharp Parker), SAGE Publications Inc, 2017.

♦ **Мусаев Эркин Гумбат оглы** - докторант кафедры уголовного права и криминологии по специальности уголовное право и криминология: уголовно-исполнительное (пенитенциарное) право юридического факультета Бакинского государственного университета (Азербайджан). E-mail: musayev2022@gmail.com