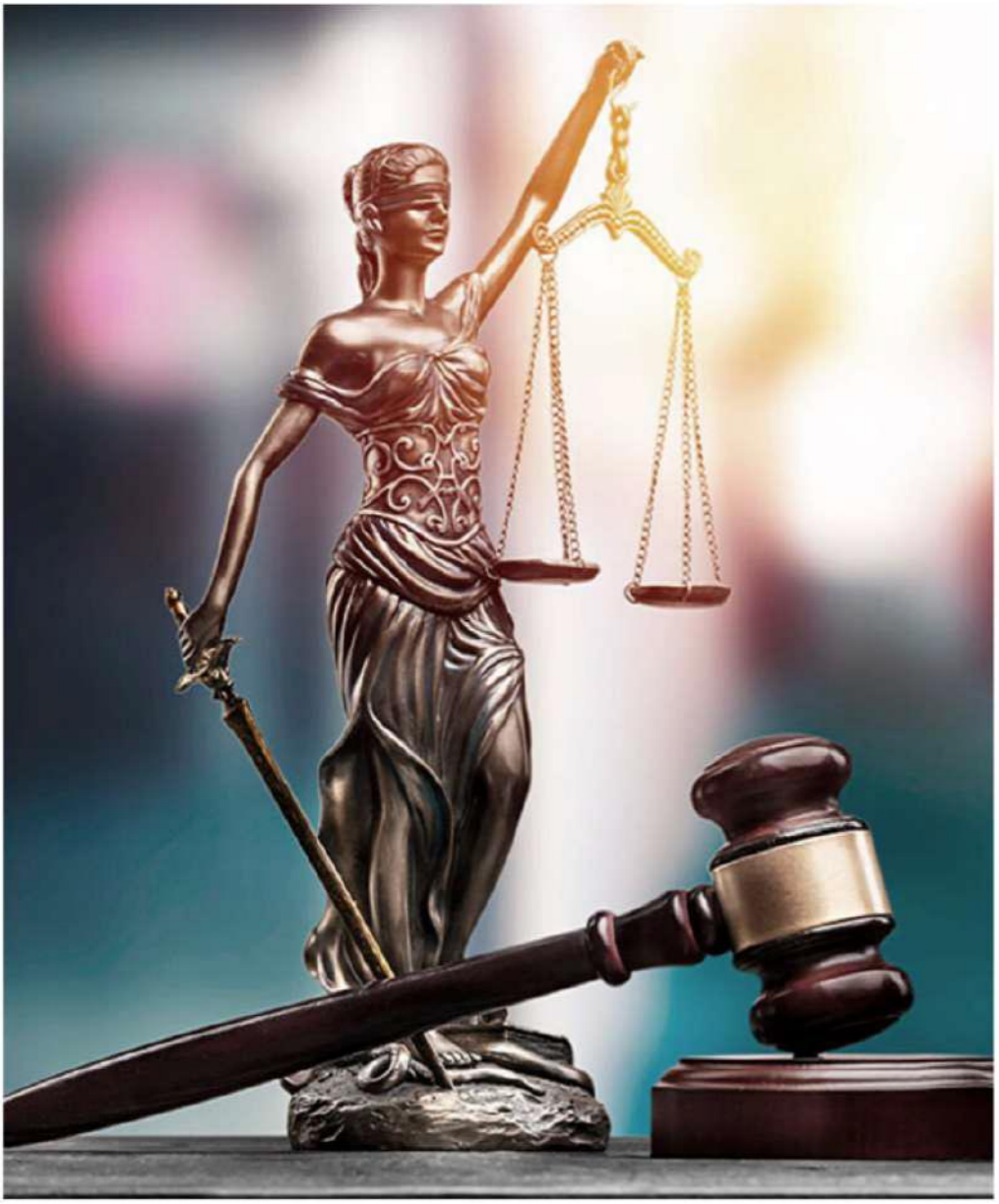
TSUL LEGAL REPORT

THE LAW JOURNAL

E- ISSN: 2181-1024



ISSUE № 1
SEPTEMBER 2020

TSUL LEGAL REPORT
T L R

ISSN: 2181-1024. Certificate: No. 1342

Contacts
Editorial office address: Tashkent, st. Sayilgoh, 35. Index 100047.
Principal Contact
Tel.: (+998 71) 233-66-36
Fax: (+99871) 233-37-48
E-mail: info@legalreport.tsul.uz

CONTENTS

12.00.09 – Criminal action. Criminalistics, investigation and search law and court expertise

TSUL LEGAL REPORT

Journal homepage: www.legalreport.tsul.uz

CYBERCRIME SUBJECT AND LIMITS OF PROOF

Rakhimova Ulzana Khamidullaevna,
Lecturer of Criminal Procedural Law Department of Tashkent State University of Law

ARTICLE INFO

Keywords:
cybercrime, subject of proof, limits of proof, sufficiency of evidence

ABSTRACT

The article deals with the issues of the subject and the limits of proof for cybercrimes. The theoretical approach to these two concepts in the criminal process is analyzed. The statistics of cybercrimes and the relevance of this problem for the entire world community are presented.

INTRODUCTION

The Internet covers our life every day. As of January 2020, Northern Europe ranked first by region with 95 percent online penetration, followed by Western Europe with 92 percent. The global average penetration rate was 59 percent, up from 35 percent in 2013 [1]. In this regard, the so-called cybercrimes committed with the help of information technology have become more frequent. Every year, criminals are becoming more sophisticated and commit "smart" crimes that require certain skills and abilities rather than physical strength. This became relevant during the coronavirus pandemic, when at least a quarter of the world's 7.8 billion people were forced to stay at home [2]. However, the crime rate did not fall, and in some countries even increased [3]. This is especially true of cybercrimes committed using information technology.

Foreign and national scientists disagree on the name of this type of crime. In science and legislation of

different countries, there are such names as “computer crimes”, “crimes in the field of security of the circulation of computer information”, “crimes in the field of high technologies”, “information crimes”, “cybercrimes, crimes in the field of computer information”, etc.

One of the first attempts to define the terms used in this area was the Agreement on Cooperation of the member states of the Commonwealth of Independent States in the fight against crimes in the field of computer information, signed back in 2001 in Minsk.

According to Art 1 of the specified document "crimes in the field of computer information" is a criminal offense, the subject of the encroachment of which is computer information [4].

Repin and Afanasyev in their article give the following brief classification of IT incidents and methods of cybercrimes:

1) leakage of confidential information;
2) illegal access to information;
3) removal of information;
4) information compromise and sabotage;
5) IT fraud;
6) abnormal network activity;
7) abnormal behavior of business applications;
8) the use of company assets for personal purposes or in fraudulent transactions;
9) Denial of Service (DoS) attacks, including distributed attacks (DDoS);
10) interception and substitution of traffic;
11) phishing, hacking, attempted hacking, scanning the company's portal;
12) network scanning, attempted hacking of network nodes, virus attacks;
13) anonymous letters (letters with threats);
14) posting confidential / provocative information on forums and blogs [5].

Today, cybercrime is becoming more widespread, and the associated illicit financial turnover reaches trillions of dollars. In 2015, Intel calculated the probable annual cost of cybercrime to the global economy at over $ 445 billion, including benefits to criminals and costs to companies to recover and protect. According to conservative estimates, the losses will amount to $ 375 billion, and the maximum - $ 575 billion [6]. The UN figures are also close to these figures. According to the UN calculations, revenues from cybercrustations in 2016 amounted to $ 445 billion, in 2018 $ 1.5 trillion, in 2019 $ 2.5 trillion. This indicator is projected to reach USD 6 trillion by 2021 [7].

To prevent and counter cybercrime, the international community has taken many actions and adopted several important international acts, such as the Bangkok Declaration “Engagement and Response: Strategic Alliances in Crime Prevention and Criminal Justice”, adopted at the 11th UN Congress in 2005, The Okinawa Charter on the Global Information Society, adopted by the G8 Heads of State and Government on July 22, 2000, Salvador Declaration on Comprehensive Strategies for Responding to Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World, adopted by UN General Assembly Resolution 65/230 on 21 December 2010.

Undoubtedly, the Budapest Convention on Cybercrime, adopted by the Council of Europe on November 23, 2001, remains an important one to this day. By the end of February 2020, 106 (or 55%) of UN members had domestic legislation criminalizing crimes against and with computers in general in accordance with the Convention. Significant progress has been noted, particularly in Africa [8]. Uzbekistan criminalized crimes in the field of information and added Chapter XX1 to the Criminal Code by the Law of the Republic of Uzbekistan "On Amendments and Additions to Certain Legislative Acts of the Republic of Uzbekistan in Connection with Increased Liability for Committing Illegal Actions in the Field of Informatization and Data Transmission" dated December 25, 2007 № 137.

MAIN BODY

It is always difficult to prove cybercrimes due to the fact that these types of crimes have high latency and in most cases it is difficult to investigate them due to many objective factors, such as the incompetence of law enforcement officers in the field of high technologies, the unwillingness of victims to tell the justice authorities about it, insufficient or inadmissible evidence in court, not falling under the jurisdiction of the victim country, which may complicate the capture of criminals and the conduct of investigative actions in general. Some also note the difficulty of preserving the evidence base, since most often computer crimes in the field of fraud are committed by large organizations, and when one criminal is caught and only one electronic device is seized, the other members of such an organization can take measures to destroy the remaining evidence confirming the

commission of other episodes or their involvement in a crime [9].

As we have already said, in the Republic of Uzbekistan, the legal basis for combating cybercrimes is laid down in the Criminal Code of the Republic of Uzbekistan, in which chapter XX1 "Crimes in the field of information technology" appeared, which includes the following corpus delicti:

- Article 278^1. Violation of the rules of informatization;
- Article 278^2. Illegal (unauthorized) access to computer information;
- article 278^3. Manufacturing for the purpose of marketing or marketing and distribution of special means for obtaining illegal (unauthorized) access to a computer system, as well as to telecommunication networks;
- Article 278^4. Modification of computer information;
- Article 278^5. Computer sabotage;
- Article 278^6. Creation, use or distribution of malicious programs;
- Article 278^7. Illegal (unauthorized) access to the telecommunications network.

However, information technology crimes are not limited to computer information crimes. In a number of compositions of the Criminal Code of the Republic of Uzbekistan, the corresponding constructive or qualifying signs of the commission of a socially dangerous act using computer technology, telecommunication networks, and also the world information network Internet are fixed.

An example is clause "d" of part 3 of article 167 of the Criminal Code of the Republic of Uzbekistan, namely theft by embezzlement or embezzlement of someone else's property entrusted to the guilty person or under his jurisdiction "using computer equipment."

Based on this, we can talk about two directions: 1) the investigation of crimes in the field of computer information and 2) the investigation of crimes, where computer technologies are used to commit other crimes. Another example of the second point is computer fraud, the so-called "online fraud".

Establishing the truth in criminal cases is impossible without defining the subject and limits of proof. Previously, these two concepts were identified, but many authors do not agree with this opinion and consider it erroneous. According to A.R. Belkin, the subject of proof is the totality of the circumstances proved in the case.

“As a result of informational reflection in the structure of knowledge of the investigator, prosecutor, lawyer, judge, as a component of consciousness, a certain place is occupied by the knowledge of the

schema of the subject of evidence contained in the criminal procedure law. This knowledge appears as a result of studying the text of the law and criminal procedural literature and generalizing their own experience in the investigation, consideration and resolution of criminal cases. In view of this, in the minds of these subjects of cognition, the subject of proof does not exist in the form of a bare scheme, but is a complex mental formation, consisting of ideas, concepts, judgments" [10].

The subject of proof (or the circumstances to be proven) is the totality of facts to be established for the correct resolution of the criminal case. A clear definition of the subject of proof in a criminal case is a necessary condition for knowing the truth and the correct legal qualification of the committed act [11, P.6]. The scope of proof is understood as the actual scope of proof, i.e. necessary and sufficient, from the point of view of the official who makes a decision in the course of the proceedings on the case, the level of research of information that establishes the circumstances to be proved in the case. The limits of proof are an essential characteristic of the proof process. After all, they reflect quantitative and qualitative changes in knowledge about the circumstances of the case; disclose cognitive activity (primarily the court) in the dynamics of its development to achieve reliable knowledge [11, P.10].

The subject of proof is a set of circumstances stipulated by the criminal procedural law that are to be established in the course of criminal proceedings by means of evidence, in order to resolve it lawfully, reasonably and fairly [12].

Alexandrov A.S. and Frolov S.A. write: “If the subject of proof answers the question of the direction of the proof, then the limits of proof speak of the means of ensuring the reliability of knowledge of the facts and circumstances that are the subject of proof [13]. Sheifer S.A. in his scientific work cites the opinion of V.D. Arsenyev, who noted that the subject of proof is data about the real circumstances of the event that has occurred, to establish which the evidentiary activity in a criminal case is aimed, i.e. information about them held by the investigator and the court. According to Schafer himself, the subject of proof is a specific procedural designation of the subject of knowledge in a criminal case. These are such objectively existing properties and connections, i.e. the factual circumstances of the event under investigation, which have legal significance, characterize it as a

socially dangerous and criminally punishable act, and the person who committed the act as a guilty [14]. In other words, the subject of proof is the totality of the circumstances provided for by the criminal procedure law that must be established for a quick, complete and fair resolution of a criminal case.

It should be noted that in order to make the correct decision in a criminal case, it is necessary that all the circumstances that are important for its resolution are reliably clarified in the course of the proceedings. For each case, only the circumstances inherent in it will be significant. At the same time, all crimes, as unlawful socially dangerous acts, contain a common thing, and each individual crime contains the same basic legal elements as other crimes. Therefore, the Criminal Procedure Code defines a number of circumstances common to all criminal cases, which are subject to proving in each criminal case (Article 82 of the CCP).

So, article 82 of the Criminal Procedure Code of the Republic of Uzbekistan lists the grounds for accusation and conviction. In order to bring a case to court with an indictment or indictment and for a conviction, it must be proven:

1) the object of the crime; the nature and amount of harm caused by the crime; circumstances characterizing the personality of the victim;

2) the time, place, method, as well as other circumstances of the commission of the crime specified in the Criminal Code; the causal relationship between the act and the socially dangerous consequences that have occurred;

3) the commission of a crime by this person;

4) commission of a crime with direct or indirect intent or through negligence or arrogance; motives and goals of the crime;

5) the circumstances characterizing the personality of the accused, defendant.

However, based on the characteristics of cybercrimes, it can be concluded that this list is not exhaustive. In this case, the following circumstances should be established:

1) the fact of the commission of a criminal act, i.e. whether the act or omission in question is criminal;

2) subject of criminal encroachment - cybercrime is not limited to computer information;

3) the place of the crime is one of the most important conditions, since according to statistics, about 70% of cybercrimes cross national borders.

4) the way the crime was committed;

5) the operating mode of the computer system or the conditions of

access to computer information, protection means;

6) traces left by the crime. Detection, fixation and seizure of traces of a crime is one of the important conditions for a legal and fair investigation of a criminal case and the collection of the necessary evidence base;

7) the nature and extent of damage can be expressed in property, physical and moral damage, as well as in causing damage to business reputation;

8) the identity of the person who committed the crime. Establishing this condition is a little difficult due to the high latency of cybercrime; 9) reasons and conditions contributing to the commission of a crime.

In accordance with the Convention, the object of cybercrimes is the public relations protected by legal norms arising in the implementation of information processes regarding the production, collection, processing, accumulation, storage, search, transmission, distribution and consumption of computer information, etc.

The object is public relations to ensure the security of computer information (inviolability of computer information), as well as the procedure for using automated data processing systems.

We can say that the object of crimes in the field of computer information has all the features inherent in the general object of the crime, the generic object of crimes against public safety and public order, the specific object of criminal attacks of the group in question, and there is also an additional feature that individualizes the object of crimes in the field of computer information and indicating that the crimes belong to the investigated group of criminal encroachments.

Thus, the object of crimes in the field of computer information is public relations protected by criminal law, which incorporate all the signs of a common object of crime, as well as limited by the nature of public relations that ensure public safety and public order, and, finally, constituting the essence of a specific and immediate object - public relations ensuring the safety of computer information.

Therefore, in the general concept of corpus delicti in the field of computer information, the first of the signs that characterize the object of the crime is the object itself, which is social relations that ensure the safety of computer information [15].

The next obligatory feature related to the scope of the object in the general concept of the corpus delicti of cybercrimes is the so-called

intangible subject of the crime. It is computer information protected by law, which exists before the start of criminal influence on it in a certain state.

The objective side of cybercrimes is characterized by the allocation of four groups of socially dangerous acts:

1. Against the confidentiality, integrity and availability of computer data and systems;
2. Associated with the use of computers;
3. Content related data;
4. Associated with violation of copyright and related rights.

From the objective side, these crimes are expressed in:

- creation, implementation and operation of information systems, databases and data banks, systems for processing and transferring information, authorized access to information systems without taking established protection measures, which caused major damage or significant harm to the rights or legally protected interests of citizens, or state or public interests (article 278^1 of the Criminal Code);
- illegal (unauthorized) access to computer information, if these actions entailed the destruction, blocking, modification, copying, or interception of information, disruption of the computer, computer system or their network (Art. 278^2 CC);
- manufacture for the purpose of marketing or marketing and distribution of special software or hardware for obtaining illegal (unauthorized) access to a protected computer system (Article 278^3 of the Criminal Code);
- unlawful modification, damage, erasure of information stored in a computer system, as well as the introduction of deliberately false information into it, causing major damage or significant harm to the rights or legally protected interests of citizens, or state or public interests (Article 278^4 of the Criminal Code);
- disabling someone else's or service computer equipment, as well as the destruction of a computer system (Article 278^5 of the Criminal Code);
- creating computer programs or making changes to existing programs for the purpose of unauthorized destruction, blocking, modification, copying or interception of information stored or transmitted in a computer system, as well as the development of special virus programs, their deliberate use or distribution (Article 2786 of the Criminal Code).

Cybercrimes are more often committed for economic purposes. This can be, for example, causing economic damage in the form of theft

of money and confidential information. Other types of goals include political goals - causing damage to basic state and political institutions, undermining the system of power relations and trust in power. The third type of ideological goals: the dissemination of ideas and ideologies with the aim of recruiting Internet users into the ranks of, for example, radical terrorist and nationalist groups. The fourth type of goals includes socio-psychological goals, such as causing moral, psychological harm to citizens.

The subject of these crimes may be a sane person who has reached the age of 16, who has committed the above criminal offenses. Attackers can be conventionally divided into several groups: hackers, spies, terrorists, corporate raiders, thieves, etc. Usually, these are people with extraordinary abilities and special knowledge in the field of computer technology. Or it is a person who has access to the operation of the mentioned technical means. These can be programmers, computer operators, service technicians, and other persons who have access to them at work.

The subjective side of the crime is characterized by intent, negligence and with a complex form of guilt, and the crimes under Art 278^3, 278^5 and 278^6 of the Criminal Code of the Republic of Uzbekistan can be committed only with direct intent. It should be noted that when committing a cybercrime, a person realizes the social danger of an act, foresees the onset of consequences harmful to society or an individual, and wants these consequences to occur, or is indifferent to them. Cybercrimes prevent them from being committed through negligence or frivolity.

CONCLUSION

Summing up, we can conclude that the subject and limits of proof are interdependent, but not equivalent concepts. The subject of proof is information about the real circumstances of the event that took place, to establish which the evidentiary activity in a criminal case is aimed. Limits of proof - this is a sufficient body of evidence that serves as a comprehensive, complete and objective establishment of all the circumstances that are relevant to the case.

Determination of the limits of proof depends on a specific criminal case and ensures the establishment of the sufficiency and reliability of evidence for making a specific decision. The difficulty is that it is impossible to establish in advance the range of circumstances included in the subject of proof in a particular case.

The circle of these circumstances is determined and established by the official conducting the investigation of the case, developing and checking versions of the event that took place. To effectively combat cybercrimes, it is necessary to create a whole system of cybersecurity, which, in addition to countermeasures, should also include an increase in the level of digital literacy of the population.

From the above, we can conclude that cybercrime is by far the most dangerous and rapidly gaining momentum problem, which must be dealt with not only at the national but also at the international level.

REFERENCES

1. https://www.statista.com/statistics/269329/penetration-rate-of-the-internet-by-region

2. https://www.bbc.com/russian/news-52034816

3. https://acca.media/uzbekistan-za-vremya-karantina-prestuplenij-v-strane-gorazdo-stalo-bolshe/

4. Fedorovich V. Yu. What is “cybercrime”? // Bulletin of the Moscow University of the Ministry of Internal Affairs of Russia, № 3, 2020 - p. 15-17

5. Repin M. Ye., Afanasyev A. Yu. Crimes in the field of computer information: problems of detection and disclosure - "Young Scientist" № 15 (95) August, 2015 - pp. 460-463

6. Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II; Center for Strategic and International Studies - June 2015 McAfee. [Электронный ресурс] URL: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/attachments/140609_McAfee_PDF.pdf

7. https://news.un.org/ru/interview/2019/10/1366141

8. https://www.coe.int/en/web/cybercrime/-/global-state-of-cybercrime-legislation-update-

9. Kaigorodova AA Topical issues of investigation and proof of cybercrime // Evolution of Russian law. Materials of the XVII International Scientific Conference of Young Scientists and Students. - Ural State Law University. Yekaterinburg, 2019 - pp. 568-569

10. A.A. Kukhta. Proving the Truth in Criminal Procedure

11. A.Kh. Garifulina and others. Proof in a criminal case. Schemes and tables: Textbook. manual - M.: UNITY-DANA: Law and Law, 2012.

12. Alferov V. Yu., Grishin AI, Ilyin NI, Chernyshev BV Fundamentals of the theory of evidence in criminal proceedings in Russia: textbook. manual - 2nd ed., revised, and add. - Saratov: Saratov Socio-Economic Institute (branch) of the PRUE. G.V. Plekhanova, 2017 .- p. 27

13. Borulenkov Y. P. The concept of "limits of proof" must correspond to the concept of adversarial proceedings // Bulletin of the Academy of the Investigative Committee of the Russian Federation. - 2014. - № 1. - P. 39-40

14. Sheifer S.A. Evidence and proof in criminal cases: problems of theory and legal regulation. M .: NORMA-INFRA-M, 2012 - P. 42

15. https://cyberleninka.ru/article/n/obektivnye-i-subektivnye-priznaki-v-obschem-ponyatii-sostava-prestupleniy-v-sfere-kompyuternoy-informatsii