**Volume 1 Nomor 5 May 2024**
E-ISSN: 3032-1298
https://economic.silkroad-science.com/index.php/IJBLPS

# PROBLEMS OF PREVENTING CRIMES COMMITTED USING THE INTERNET

**Allanova Azizakhon Avazxonovna,**
Professor of the Department of Criminal Law, Criminology and Anti-corruption
Department of Tashkent State University of Law, PhD in Law
E-mail: aziza9106@mail.ru

**Article Info**

***Article history:***
Received June 05, 2024
Revised June 25, 2024
Accepted July 05, 2024

***Keywords:***
Cyberspace, internet network, crime, crime prevention, causes and conditions

**ABSTRACT**

This scientific article describes the problems of preventing crimes committed using the Internet, crime prevention, the specific characteristics of crimes committed in cyber space, the analysis of crimes committed using the Internet in the criminal laws of some foreign countries.

**Corresponding Author:**
**Allanova Azizakhon Avazxonovna,**
Professor of the Department of Criminal Law, Criminology and Anti-corruption
Department of Tashkent State University of Law, PhD in Law
E-mail: aziza9106@mail.ru

## INTRODUCTION

Crime prevention is a complex of measures implemented by state bodies and the public at different levels to prevent crime, eliminate its causes and conditions. The problems of preventing crimes committed using the Internet network can be said to be a set of circumstances that hinder the minimization or termination of crimes committed in this area. These, in turn, are divided into several types.

As for the legal factors, the imperfection of the National Criminal Law in the field of combating crimes committed using the Internet is included. Until now, the issue of calculating the damage caused by criminal aggression related to this type of crime has not been finally resolved in the criminal, administrative and civil legislation. In addition, there is not enough practice in the courts regarding the consideration of this type of crime by the courts, and there is no Plenum decision by the Supreme Court on the sentencing of this type of crime. This creates problems for judges to issue fair and correct sentences for crimes committed using the Internet.

Political factors include the lack of effective control over cyberspace and the media. Today, the Internet is not fully controlled or owned by any country, meaning that anyone can engage in legal or illegal activities on the Internet without permission, simply by using the technology to access the Internet. existence is sufficient. Due to the lack of self-control, no organization or state controls the Internet, crimes can be committed by Internet criminals at any time

## METHODS

Descriptive analysis and case study methods to explain the problems in cybercrime prevention. This method involves identifying and evaluating various factors that affect cybercrime prevention, such as deficiencies in national criminal laws, political constraints, globalization, and extraterritoriality, as well as technical issues and digital culture. By exploring existing problems and providing specific examples of ongoing cybercrime, this article presents a comprehensive picture of the challenges faced and urges the need for legal reform and awareness-raising to deal with cybercrime.

## RESULT AND DISCUSSION

Entering the stage of globalization of modern society into social factors. According to preliminary data, the number of Internet users in the Republic of Uzbekistan has reached 30 million. This is 80-90 percent of the 36 million people living in Uzbekistan, thus Uzbekistan ranks first in the number of Internet users in Central Asia. And this number continues to grow day by day, which in turn leads to an increase in social relations on the Internet, and ultimately to an increase in Internet crime, unfortunately, in this case, it is impossible to stop globalization, it is on the one hand while giving the opportunity to solve some problems for humanity, on the other hand, it is causing the problems arising through them to increase. The Jurisdiction Problem The primary challenge to jurisdiction is that the Internet is borderless and there are no territorial boundaries to cyberspace. This is because the location of the victim and the location of the perpetrator are unclear. There are no international standards on cyberspace jurisdiction. It's such a gap that you can't control it.

The extraterritoriality of cyberspace is a determining factor in the existence of economic cybercrime. Because crimes committed using the Internet are often global and transnational in nature, they span multiple jurisdictions. A.V. Susloparov emphasizes that the peculiarity of computer crimes is their international character. They can be done in different places around the world. At the same time, it does not matter in which country the object of criminal aggression is located for the Internet criminal. In fact, the distance between the perpetrator and the victim can be from several meters to several thousand kilometers, although in cyberspace they can be regular visitors of the same site or social network. At the same time, the number of victims of one cybercrime can be dozens or hundreds, and they, like the criminals themselves, can live in different countries of the world. From the subjective point of view, the criminal considers the act of stealing money from a foreigner electronically or without cash or deceiving a citizen of another country to be socially insignificant. Cyberspace itself is extraterritorial - it has no borders, no countries, but there sites, forums and their users can be deceived or their property stolen. This problem greatly complicates the investigation, proof work, extradition process and creates the problem of bringing the act to criminal responsibility. Some economic crimes committed in cyberspace are not prosecuted in Uzbekistan or are considered an administrative offense. The opposite is also possible: socially dangerous actions considered criminal in Uzbekistan may not be so in other countries.

If we look at the example of the USA, the United States has extradition treaties with more than 100 countries. It is possible to get criminals from these countries, but it is not 100 percent guaranteed. Governments may choose not to extradite in any case. For example, the United Kingdom chose not to extradite Laurie Love to the United States in 2018 due to mental health issues. More than 76 countries do not have extradition treaties with the United States. This means that even if the perpetrator is known, they are less likely to be prosecuted.

Cyberspace is technically imperfect and contains technical weaknesses, loopholes and simple errors. in which it repeals almost all countermeasures against cybercrime. As such gaps, the following example can be given: when materials of an extremist nature are found on the site, the authorized body in Uzbekistan includes this site in the list of extremist sites. However, any user, including the Uzbek segment of the Internet, can use extremist sites in ways that circumvent this ban, and software vulnerabilities allow unauthorized access to all sites. This issue has received very little attention both from the legislator and from the scientific point of view. Legal measures are being taken hastily without considering this issue. Although many services such as Internet commerce and Internet banking are provided, little attention is paid to their safe operation.

There are no rules of conduct in cyberspace, so many site or forum administrators are forced to invent their own. The lack of uniform and clear rules of conduct in cyberspace leads to the emergence of many new subcultures, such as hackers and cybercriminals. The administration can be limited by warnings, access restrictions and blocking ("ban") access to the resource. Such sanctions are ineffective, because there are a lot of similar sites in cyberspace, and if the violator is blocked on one site, he can freely register on another or re-register on a blocked site under a different name. In this regard, it is more effective to block the IP address, not the user, but this ban can be bypassed through special programs or by accessing from other devices.

Therefore, the lack of a minimum level of digital literacy and culture is one of the main problems in preventing cybercrimes. The habit of checking computer viruses, not visiting suspicious sites should be developed among citizens at the same level as the habit of washing hands before eating and not starting a conversation with strangers. These are elementary precautions that are often forgotten in cyberspace. The only effective solution to this problem, in our opinion, is to prevent information security among the population. The basic rules of behavior in cyberspace should be inculcated from an early age, for example, through special training in high school.

Law enforcement officers are primarily unskilled in the cybercrimes they encounter, and lack the necessary knowledge to find and prosecute perpetrators, which leads to a high level of cybercrime latency.

At the press conference held at AOKA with the participation of the employees of the Cyber Security Center of the Ministry of Internal Affairs of the Republic of Uzbekistan, it was announced that a number of analyzes were conducted. The results of the analysis showed that the country is currently experiencing an increase in cybercrime, and that the number of cybercrimes has increased several times over the last 3 years. According to the press conference, it was reported that the following types of cybercrime are being committed:

– Fraudsters have come to plastic card users

– Taking the codes in the SMS-message under the pretext of making a payment, awarding a prize, and embezzling the funds from it;

- extortion by threatening to acquire and disclose personal data (cyber extortion);
- bullying, insults, cases of suicide (cyberbullying) on social networks, etc.

From the above information, we can see that the crimes committed in cyberspace are different from traditional crimes such as extortion and suicide. But these cybercrimes are not directly defined in our legislation, but they are the most committed acts. This situation clearly shows that legislation cannot develop simultaneously with cybercrimes. It is not wrong to say that perfecting legislation in cyberspace is a very urgent problem.

## CONCLUSION

The study underscores the multifaceted challenges in combating cybercrime, revealing significant gaps in legal frameworks, political control, and technical measures. Findings highlight the inadequacy of national legislation in addressing the complexities of cybercrimes, which are often transnational and extraterritorial. The lack of effective jurisdictional standards and the technical vulnerabilities of cyberspace further exacerbate these issues. Implications suggest an urgent need for legislative reform and enhanced international cooperation to address the borderless nature of cybercrime. Additionally, increasing digital literacy and developing robust cybersecurity practices are critical for prevention. Further research should focus on developing international legal standards and effective technological solutions to bridge these gaps and improve cybercrime response mechanisms.

## REFERENCES

[1]. A. V. Susloparov, "Some Directions for Improving Legislation on Liability for Computer Crimes Considering International Experience," Ministry of Education and Science of the Russian Federation, Tambov State University named after G.R. Derzhavin, Ed. A. V. Shunyaeva, E. A. Popova, S. A. Puchnina, Tambov: Publishing House of TGU named after G. R. Derzhavin, 2013, p. 105.

[2]. "Prosecuting Cybercrime: Challenges," Cipher, [Online]. Available: https://cipher.com/blog/prosecuting-cybercrime-challenges/. [Accessed: Aug. 28, 2024].