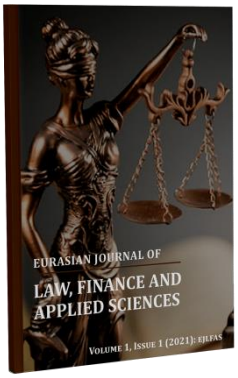
EURASIAN JOURNAL OF LAW, FINANCE AND APPLIED SCIENCES
Innovative Academy Research Support Center
UIF = 8.3 | SJIF = 5.961 www.in-academy.uz



DETERMINATION OF THE JURISDICTION LEGAL STATUS OF INDIVIDUAL PERSONS AS SUBJECTS IN CYBER SPACE

Dadajonov Jahongir Qobiljon o'g'li
Master of Faculty of Cyber law of TSUL
https://www.doi.org/10.5281/zenodo.10517339

ARTICLE INFO

Received: 08th January 2024
Accepted: 15th January 2024
Online: 16th January 2024

KEY WORDS

Cyberspace, jurisdiction, cyber activity, cybercrime.

ABSTRACT

This article explores the topic from different perspectives, in particular, it examines the legal framework governing cyberspace, jurisdictional issues, problems and potential solutions related to the civil and criminal legal rights and obligations of its subjects in the virtual world. In order to increase the accuracy of these data, various statistics and legal documents were widely used. Within the scope of the topic, targeted references were given from the opinions of foreign and national scientists, scientific works, research results, newspapers and magazines, legal documents of foreign countries.

INTRODUCTION

In the 21st century, the rapid growth of the Internet and the spread of digital technologies, while bringing convenience to social life and people's lifestyles, at the same time, are creating many problems for legal systems around the world. Due to the fact that people's interactions are increasingly moving to the virtual world, there is a need to understand and define the civil and criminal legal status of individuals in cyberspace. Therefore, there are gaps in the regulation of this activity in society.

METHODOLOGY

The purpose of this study is to analyze the status of cyberspace and its subjects, the role of the parties in the performance of legal obligations and other aspects of their relationship as subjects in the legal system. The main thing is to reveal that their level of subjectivity has a civil and criminal legal status as the subjects of existing national or international law or different.

To achieve these goals, the author compares scientific research used several methods such as sociological analysis, synthesis, comparative.

RESEARCH RESULTS AND DISCUSSION

Basically, cyberspace refers to a virtual environment created by computer systems and networks where individuals can interact, share information, and engage in various activities. Instead, it encompasses the Internet, online platforms, social media, and other digital spaces, and opinions vary about cyberspace and its impact on society. Cyberspace has often been

analyzed by scholars as a non-legal domain or address on the internet. In particular, in **John Barlow's** Declaration of Cyberspace Independence, the view that ***"legal concepts specific to real life do not apply to cyberspace"*** is put forward.[1] This view of cyberspace as a non-legal territory is based on a number of assumptions. The first assumption is that, according to **David R. Johnson and David G. Post [2],** cyberspace is territorial, borderless, and ubiquitous, and differs from the real legal world in which the legal system has regulatory and subordinate principles. Second. the assumption is that, according to **Tim Wu and Jack Goldsmith**, **[3]** cyberspace should retain its original concept of being an open, decentralized and participatory space, unencumbered by legal norms. Nevertheless, the view that Cyberspace is subject to law and indeed international law has come to a certain halt. According to a comparative analysis, most scientists engaged in scientific research emphasize that in cyberspace, as in the real world, there should be a system that determines the legal order of jurisdiction and the actions of subjects in it. Below are the legal grounds for determining the subjectivity of cyberspace subjects by determining whether their actions belong to different jurisdictions based on various national and international legal norms.

The role of the national legislation of states in determining the legal status and jurisdiction of an individual in cyberspace. In particular, many groups of experts in the field of information and organizations in the field of telecommunications envisage the application of international law and the UN Charter to cyberspace, the principle of state sovereignty and the application of international norms to relations arising from this field. In addition, the supporters of this idea put forward the idea that wherever the infrastructure operating in cyberspace is located, all its actions in the virtual world are subject to the jurisdiction of this state.[4] Therefore, jurisdiction serves as the largest legal basis in determining the legal status of individuals, which is one of the most complex and developing legal areas of cyberspace. Jurisdiction in cyberspace is difficult to determine because the physical locations of servers, data, and participants are spread across different countries, and the rules of jurisdiction vary from country to country. For this reason, conflicts can arise when multiple jurisdictions claim the same dispute.[5]] In general international law, one of the main factors determining the jurisdiction to determine the status of a natural person, who is considered the main subject of cyberspace, is his citizenship and place of residence.[6] In this case, any actions of a person, regardless of where the action takes place, are regulated by his national legislation. We understand this provision to mean that if a person is a citizen or resident of a particular country, the laws of that country may apply to their actions, even if they are conducted online or outside the country's territorial borders. This practice can mainly apply to activities such as cybercrime, online fraud, or distribution of illegal content.[7] For example, if a US citizen living in Germany engages in online activities that are illegal under US law, they can still be prosecuted by US authorities. Analyzing the practice of other countries according to this principle, almost all of their existing legal norms for the regulation of the cyberspace contain this provision. . In particular, **in Article 9 of this law**, "the provisions of this law, *against any person within the jurisdiction of Malaysia, whether a citizen or a non-citizen, both outside and within Malaysia, and if an offense under this Act is committed by any person outside Malaysia even so, it can be treated in the same way as it is treated in relation to a crime committed within Malaysia."[8]* Extraterritorial jurisdiction

allows states to assert their authority beyond their geographic boundaries. The state can exercise jurisdiction not only over cyber structures and citizens engaged in cyber activities located in its territory, but also over stateless persons located in its territory.[9] Such an approach raises questions of sovereignty and conflicting legal frameworks and often leads to international legal disputes.[10] This principle ensures that individuals cannot avoid legal consequences by taking advantage of the anonymity or borderless nature of the Internet. The important aspect of this theory is that the legal responsibility of individuals is determined mainly by their national legislation. This rule also has certain endpoints, as a result of the spread of legal behavior of a person across borders and social relations with representatives of different nationalities, as a result of which his legal rights and obligations are tied to the legislation of another state, his legal status also directly affects his actions. In some cases, the person's physical location at the time of the offense or the location of the server hosting the content may determine which state the person is subject to jurisdiction. If a person commits a cybercrime within the borders of a certain state, that state has the power to prosecute the person.[11] That is, this principle is built on the basis of territoriality, the consequences of its actions, the starting point and other aspects are taken into account, and on this basis the question of the responsibility of the person is solved. There are several other legal approaches to dealing with territorial jurisdiction in cyberspace, which attempt to strike a balance between protecting individual rights and ensuring the continuation of the legal order in the digital realm. determined by the location of the damage caused or the effect of the action in question. It relates to persons whose actions have a significant connection with a particular jurisdiction, regardless of their physical location. So, as the cyber activity of a natural person expands, the definition of his rights and obligations also changes.

Determining the jurisdiction of entities in cyberspace through international legal cooperation. Due to the transnational nature of cyberspace, international cooperation and treaties play a crucial role in the exercise of jurisdiction over the determination of the legal status of individuals. In particular, mutual legal assistance agreements facilitate cooperation between governments to share evidence and information for cross-border investigations. International cooperation in cyberspace is mainly devoted to the issue of prevention of cybercrimes and responsibility towards the subjects of cybercrime, because in this type of crime, subjects commit cross-border crimes and the quality of transnational crime against individuals is different due to the fact that its starting point and the point of consequence are in different regions of the world. In particular, by the representatives of the Council of Europe, the adoption of relevant legislation on cybercrime and the development of international cooperation, the general criminal policy aimed at protecting society from cybercrime as a priority, the deepening of the digitalization of computer networks, convergence and the continuation of globalization 2001 in order to prevent the negative consequences of the changes, to establish cooperation on the possibility of using computer networks and electronic data to commit criminal offenses and the risk of evidence of such offenses being stored and transmitted by these networks, 2001 On November 23, the convention was adopted in Budapest. It mainly includes several types of cybercrimes, such as illegal access to a computer system, illegal access to computer data, and misuse of devices. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal entities

recognized in accordance with this Convention are held accountable for criminal offenses committed by any natural person acting alone or as part of its own interests. Sees. **Article 22 of the Convention** provides the following procedure for determining jurisdiction over persons who are subjects of cyberspace:

Each Party shall take such legislative and other measures as may be necessary to establish jurisdiction over any crime established in accordance with the articles of this Convention, if the crime:

a. in its territory;

b. on board a ship flying the flag of that party;

c. on board an aircraft registered under the laws of that country;

d. by one of its nationals, if the offense is punishable under the criminal law of the place where it is committed, or if the offense is committed outside the territorial jurisdiction of any State,

Each party may reserve the right not to apply or to apply the jurisdiction rules set forth in paragraphs 1.b through 1.d of this article or any part thereof only in certain cases or circumstances. Each Party shall, if the suspected criminal is in its territory and does not hand him over to another after a request for extradition, take the necessary measures to establish jurisdiction on the basis of his nationality for the offenses referred to in Article 24, paragraph 1, of this Convention. takes appropriate measures.

This Convention does not exclude criminal jurisdiction which a Party may exercise in accordance with its domestic law.

If more than one party claims jurisdiction over an offense established under this convention, the parties involved shall consult to determine the most appropriate jurisdiction for prosecution.[12] The members of this convention mainly gave priority to the national legislation in determining the civil or criminal responsibility of their country, because they joined this convention in order to avoid the responsibility of constitutionally protecting the legal interests of their citizens, as well as various complex legal situations. At this point, the question may arise: Are there legal grounds for establishing jurisdiction over consequences arising from civil legal relations in cyberspace? The Code of Civil Procedure of almost all countries does not establish jurisdiction over the consequences of this behavior of citizens in cyberspace. In simple terms, the authority of the court to resolve this issue is to refer [13] or refer to jurisdiction as the authority granted to a formally established legal body to make decisions on legal issues and to administer justice in a designated place of control with its help. possible It is also used to describe a subject or geographic area over which authority exists.

CONCLUSION.

Taking into account that subjects in cyberspace are the subject of civil law and criminal law as a result of the consequences arising from social relations, in solving the issue of responsibility towards them, the subject belongs to the jurisdiction of which state under the sovereignty of the subject, the legal basis of regulating the actions of cyberspace subjects in local legislation, and how it is defined in international legal norms. taking into account their responsibility is determined.

References:

1. John P Barlow, 'A Declaration of Independence for Cyberspace' (Davos, 1996) <https://projects.eff.org/~barlow/Declaration-Final.html> accessed 22 July 2014.
2. David R Johnson and David G Post, 'Law and borders: The rise of law in cyberspace'(1996) 48 Stanford L Rev 1367. Contra Jack L Goldsmith, 'Against cyberanarchy' (1998) 65 U Chi L Rev 1199.
3. Tim Wu and Jack Goldsmith, Who Controls the Internet? Illusions of a Borderless World (OUP 2006)
4. Research handbook on international law and cyberspace.St. Louis: Edward Elgar publ., 2016.– P.13
5. Berkman Klein Center for Internet & Society at Harvard University: "Jurisdiction" https://cyber.harvard.edu/system/files/Faulhaber-Jurisdiction.pdf.
6. Nations specialized agency for information and communication technologies. www.itu.int
7. Jurisdiction in Cyberspace: A Theory of International Spaces. https://repository.law.umich.edu/mttlr/?utm_source=repository.law.umich.edu%2Fmttlr%2Fvol4%2Fiss1%2F3&utm_medium=PDF&utm_campaign=PDFCoverPages.
8. Sovereignty and jurisdiction https://www.unodc.org/e4j/en/cybercrime/module-7/key-issues/sovereignty-and-jurisdiction.html.
9. Миятова Сая. Распространяется Ли Суверенитет На Киберпространство? https://www.mjil.ru/jour/article/download/2246/2145.
10. https://unijuris.sites.uu.nl/wp-content/uploads/sites/9/2014/12/The-Concept-of-Jurisdiction-in-International-Law.pdf.
11. https://legalvidhiya.com/international-position-of-cyberspace-jurisdiction-2.
12. Convention on Cybercrime Budapest, 23 November 2001 https://assets.publishing.service.gov.uk/media/5a7c929ded915d6969f45d32/8309.pdf.
13. https://blog.ipleaders.in/civil-procedure-codes-application-cyberspace .