

OVERCOMING CONFLICTS OF JURISDICTION IN VIRTUAL SPACE: AN ANALYSIS BASED ON CASE LAW AND LEGAL REGULATION

Elnur Humbatov*

Abstract

Since the virtual space is a borderless space and the established rules are based on the principles of territorial sovereignty, the existing rules and principles must either be changed or new jurisdictional principles need to be created for this space. At present, a number of national courts use principles established by taking into account the interests of their territories or citizens. If any criminal behavior of an individual in the virtual space affects the citizens of many states, there is no universal international source for proportionately compensating the loss. Therefore, there is a need for international cooperation and harmonization of national legal regulations to solve jurisdictional problems in virtual space. Also, the development of common standards around the world may be of particular importance to overcome the limitations of traditional jurisdiction and ensure adequate jurisdiction in cyberspace. The issues mentioned in the article have been studied in detail, and practical suggestions for solving the jurisdictional problem in the virtual space have been presented based on court experience.

Keywords: *virtual space, cyberspace, Internet, jurisdiction, predictability requirement, human rights, international regulation.*

1.1. Introduction

As a result of the development of information technologies, today the world is experiencing a rapid digital transformation in all areas, and virtual environments have invaded our lives. Today, the use of web technologies has reached such a level that the Internet is widely used not only for information acquisition, but also for information exchange and virtual collaboration. Since 2010, thanks to the transition to Web 3.0 technology, virtual environments have been formed with the introduction of content control software. These virtual environments provide individuals with opportunities for work, education, and socialization. The virtual world, which is the most relevant topic of the era, can be considered as an environment where people are represented by avatars, where there are many users and interactions, and which simulate the physical world we live in three-dimensionally with virtual reality. In the virtual world, which enters our lives as a digital twin of the physical world, real people can present themselves in any gender and shape they want. In this case, digital identities are formed in the virtual world, where many things that can be done in the physical universe, such as shopping, education, socializing, entertainment, activities, travel, can be done in three dimensions. At the same time, the "participation" of individuals in such worlds in the desired form allows any violation of law to be committed anonymously, which is one of the dangerous problems of virtual worlds. Therefore, when virtual worlds are formed both technologically and legally, a complex human-centered approach should be guided.

The formation of virtual space is not analyzed in a positive way. In the digital age, serious changes are observed in the nature of crimes through the opportunities provided by new technologies. Violations, which are no longer on the physical plane, but on the virtual plane, cause serious concerns for the modern world population.

* Ph.D. in Law, Lecturer at the UNESCO Chair of Human Rights and Information Law at Baku State University

1.2. Virtual space, cyberspace and the Internet: different and similar features

The concept of virtual can be applied to any situation that can happen online. [1] Virtual worlds are currently understood as animated three-dimensional environments created by computer software. [2]

Virtual worlds aim to make the user feel like they belong to that world in the huge environments they offer, both in terms of space and population, and that the experience is as good as the real world. The reality technologies that we will mention below are developed to improve the experience of the virtual world by feeling the movements and feelings simulated in these environments by the user with the five senses, and the control of the user's perception of reality is carried out through these technologies.

The Internet encompasses all networks created by electronic devices at an international level. Data is transferred between networks by programs installed on computers and other smart devices, which contain files consisting of various elements, especially graphics, images and texts. The Internet acts as the largest mass communication tool, being the largest and most personalized resource among the resources that can satisfy the need for information and socialization with modern technology. [3]

The European Court of Human Rights also noted in the *Times Newspaper Ltd v. United Kingdom* case that websites greatly contribute to providing access to current affairs and facilitating the general exchange of information through their ability to store and publish large amounts of information and their accessibility. [4]

The Internet, which began to be widely used in the 1990s, is characterized by dynamic development. If we analyze in chronological order, the development of technology today allows us to exchange information with the whole world through Web 1.0, Web 2.0, Web 3.0 and Web 4.0. When Web 1.0 was released, people for the first time observed data being transferred from one point to another through a network. But this technology enabled one-way communication by only allowing people to read.

After the 2000s, with the development of Web 2.0 technology, the possibility of sharing and a common space was created for Internet users. With the development of new technology, people began to use blogs and social media effectively, which ultimately led to the formation of the virtual world. But in addition to its positive aspects, this technology brought with it many problems. Thus, the mutual exchange of information led to the spread of any information in the virtual space within seconds, so that the scattered state of the available information resulted in the "drowning" of people in the information ecology and the inability of users to find what they were looking for. Considering that all information is stored on the Internet without any selection, over time, outdated information was made available to people as a result of search, creating serious difficulties in their information selection and the use of the Internet as a whole. The development of Web 3.0 technology played an important role in preventing these problems. So, with the application of this technology, data is no longer stored on single servers, but distributed among users. Necessary computing moves from data centers to user's laptops, smartphones and smart gadgets. Most importantly, this technology supports artificial intelligence and machine learning. Smart algorithms are very useful in helping users find the content they need. At the same time, the application of the authorization method in Internet use continues to change towards a single level, which will be the key to all resources on the network. For example, almost any website can be accessed using a Google or Facebook account. More specifically, with Web 3.0 technology, the working mechanism of the Internet has become more intelligent.

W. Lambert Gardiner writes that hypermedia can perform two functions: the function of a window to the objective world and the function of a mirror of the subjective world. If the first function expresses the virtual reality and reflects the accurately perceived world, the second function covers the cyberspace and defines the exact conceptual basis of that world. [5]

It is considered that the term cyberspace is used in connection with legal issues, and the concept of virtual space is used only in connection with technical and social issues. However, this approach is likely to change in the near future with the dynamic development of virtual worlds. The development of new technologies has led to the virtualization of people, and this process is accelerating day by day.

1.3. Resolution of the issue of jurisdiction in case of violation of rights in virtual space: ways to overcome contradictions in legal regulation

In most legal systems, the law of the place where the damage occurred (*lex loci delicti*) applies. In many cases, the law of the place where the action is taken is preferred. Both options have negative consequences for the plaintiff and the defendant. If the place of action is taken as the basis, if the damage occurs in countries other than the place of action, the claimant will not be compensated for all the damages. Similarly, if the law of the place where the damage occurred applies, the defendant will not be able to foresee the law that will apply to the dispute. Therefore, in both cases, one of the parties cannot foresee the law that will apply to the dispute. In terms of balancing the interests of both parties, such an approach has been put forward that in order to apply the law of the place where the damage is inflicted, the defendant must foresee that the damage may occur in that place. [6]

But content uploaded or sent in virtual space can reach users in multiple countries within seconds. In this regard, it is very difficult to predict the damage caused by such content in advance, that is, the subject distributing the content cannot control in advance in which countries this content will be used. Social media platforms and search engines, in particular, bear an enormous responsibility in this regard. Thiede, Thomas and McGrath, Colm P. call this the chilling effect, stating that such an expanded burden of liability doubles down on legal certainty. [7] Therefore, the requirement of foreseeability should not be applied as is, but should be limited to the criterion of the purpose of delivery of the broadcast (especially in relation to the person who broadcasts the content). Accordingly, for an entity to be liable for content uploaded to the Internet, it must have intentionally distributed it. [8] This means that, most importantly, the purpose of distributing the content is investigated, and if the intent to distribute is proven, liability is established. When analyzing the demand for predictability, attention should also be paid to the victim's social connections. Because in most cases, the content is distributed in the territory of the state where it is more popular.

Lex fori is a binding point defended by the fact that the law best known and applied by the judge is his own law. Accordingly, the dispute must be resolved in accordance with the law of the court where the case is conducted. According to this opinion, the beneficiary's nationality, habitual residence and the place where his personal right was harmed are not important. If the dispute between freedom of expression and other rights affects the public sphere of a particular state, the substantive law of the state must be applied to the dispute within the sovereignty of the state in question. *Lex fori* practice is effective because the judge applies the law he already knows, and in this

regard, it is possible to conclude the court proceedings in a short time. Also, thanks to this mandatory rule, the requirement that the person causing the damage should have foreseen the damage is eliminated. In fact, the *lex fori* is not very successful in dealing with violations that occur in virtual space. This criterion is given less place in Continental European law than in Anglo-Saxon law. [9]

Let us refer to a few court cases on the jurisdictional issue. The first case is related to the company "CompuServe", which was reviewed in 1996 in Germany. In the case, the German court demanded that the US company CompuServe close access to pornographic materials. The company had to remove such material from its US central server to comply with German law. As a result, even in countries where pornographic materials are not prohibited by law (including the United States), citizens were deprived of using these materials. "CompuServe" company had to obey the strictest norms in this field. This work has created such a trend that the Internet will be subject to the most restrictive norms. [10]

In another case known as the Dow Jones Case, a company (Dow Jones & Company) published Wall Street and Barrons Magazine. The magazine was uploaded to servers located in the US state of New Jersey and contained material allegedly defamatory of the defendant, Joseph Gutnick, a resident of Victoria, Australia. The most important question raised in this case was the question of the court's jurisdiction. The court said the material was uploaded in Victoria. As such, a Victorian court has jurisdiction and Victorian law governs the rights and obligations of the parties. [11]

In 2001, in the case related to the company "Yahoo!", the issue of violation of the French legislation prohibiting the distribution of materials promoting Nazism was raised. French law prohibits citizens from accessing the site of Yahoo!, which promotes Nazism. Although that site operates in the United States, it is legal to post such material in that country. [12]

As can be seen, different jurisdictions have been established for different cases. This once again proves that gaps in international regulations require states to resolve disputes in virtual space by following their domestic legislation. But here we should especially mention that there are serious differences regarding criminal and civil jurisdiction. We should mention the Cybercrime Convention on criminal jurisdiction. According to Article 22 of the Convention, the question of which state's norms will be applied is resolved in four paragraphs. As can be seen, the Convention is based on territorial and personal jurisdiction. Thus, if the cybercrime is committed on the territory of the state, on a ship sailing under its flag, as well as on an aircraft registered in accordance with the laws of that state, this state has the opportunity to take measures to determine the jurisdiction in relation to the act. In addition, if the act is committed in the territory of another state that has ratified the Convention, but the subject is a citizen of a specific state, then the jurisdiction of that state can also be applied. However, in this case, the crime must be criminalized in the state where it was committed. In addition, the Convention establishes that if the criminal act falls under the jurisdiction of several states, then the states can hold consultations in order to choose the most appropriate jurisdiction to carry out the criminal prosecution (Article 22) [13].

As for civil jurisdiction, first of all, we should mention the Law on International Private Law, which can be applied to those norms in case of legal violations occurring in the virtual space. However, if the dispute is of an international nature, reference is

made to the international agreements that Azerbaijan is a supporter of. This rule is reflected in all legislative acts in the field of information.

1.4. Conclusion

Traditional international law does not oblige a person to obey the laws of another state as long as he does not enter the territory of another state and does not directly affect the territory of that state. But does this rule apply to the Internet age? - Currently, it is difficult to observe how many countries are directly or indirectly affected by any violation of rights in the virtual space. In order to deal with the problems caused by cyberspace in such a mixed situation, there is a need to create an international organization and formulate unified material and procedural legal norms. For this, cyberspace must first be declared *res extra commercium* (that is, an area not subject to national ownership, such as the high seas). The international organization that will be created should operate on the basis of material and procedural norms. It is true that currently a number of international regulations reflect material norms. However, procedural deficiencies and lack of procedural rules make it difficult to apply those material norms. This is especially evident in relation to crimes committed in virtual space. For example, when investigating complaints made at the domestic level in cases of fraudulent online theft of funds and illegal interference with private life, which norm will be applied is determined, but the procedural issues related to the application remain unresolved. If the person who illegally withdrew money from a person's card account is located in a country that is too far away and has different regulations, the protection of the person whose rights have been violated and the restoration of their rights are called into question. Therefore, there should be perfectly integrated national networks operating under the supervision of an international organization created for the purpose of implementing procedural norms. All this will lead to the following successful results:

- thanks to the international cooperation of states, it will be easy to prevent violations caused by using virtual space;
- the arbitrary domination of technologically powerful states over other states will end.

References:

1. Ralph Schroeder. Defining Virtual Worlds and Virtual Environments / Journal of Virtual Worlds Research, 2008, Vol. 1. No. 1. file:///C:/Users/User/Downloads/tldadmin,+Schroeder_ready_nc.pdf
2. Peter J.Quinn. A click too far: the difficulty in using adhesive American law license agreements to govern global virtual worlds // Wisconsin International Law Journal, 2010, Vol. 27, No. 4, p. 760.
3. Akgül, A. A New Right in the Protection of Personal Data: "The Right to be Forgotten" and the "Google Decision" of the EU Court of Justice. TBB Magazine, 2016, p. 26 (in Turkish).
4. Times Newspaper Ltd v. the United Kingdom, Application no. 64367/14, 13 November 2018. <https://globalfreedomofexpression.columbia.edu/cases/times-newspapers-ltd-v-united-kingdom/>
5. W. Lambert Gardiner. Virtual Reality/Cyberspace: Challenges to Communication Studies. // Canadian Journal of Communication, 1993, Vol 18 (3),<http://www.cjc-online.ca/index.php/journal/article/view/762/668>
6. Foreseeability and the Rule of Law in Data Protection after the PNR judgment // The Future of the European Security Architecture: A Debate Series, 10 May 2023. <https://verfassungsblog.de/foreseeability-pnr/>
7. Thiede, Thomas and McGrath, Colm P., Mass Media, Personality Rights and European Conflict of Laws (March 27, 2011), 22 p. p. 15. <https://ssrn.com/abstract=1964506> or <http://dx.doi.org/10.2139/ssrn.1964506>
8. Thiede, Thomas and McGrath, Colm P., Mass Media, Personality Rights and European Conflict of Laws (March 27, 2011), p.16. <https://ssrn.com/abstract=1964506> or <http://dx.doi.org/10.2139/ssrn.1964506>

9. Tekinalp, Gülören, *International Private Law Binding and Procedural Law Rules*, Vedat Kitapçılık, 13th Edition, Istanbul, 2020, p. 35 (in Turkish).

10. Aliyev, A.I., Rzayeva, G.A., Ibrahimova, A.N., Maharramov, B.A., Mammadrzali, Sh.S. *Right to information*. Textbook. Baku, Nurlar, p. 383.

11. Shelke, Atmaram and Gurple, Shashikala, *Problem of Jurisdiction in Cyberspace and its Impact on International and Domestic Laws* (December 7, 2019), p. 18. SSRN: <https://ssrn.com/abstract=3500049> or <http://dx.doi.org/10.2139/ssrn.3500049>

12. Aliyev, A.I., Rzayeva, G.A., Ibrahimova, A.N., Maharramov, B.A., Mammadrzali, Sh.S. *Right to information*. Textbook. Baku, Nurlar, p. 383.

13. *Convention on Cybercrime*, Budapest, 23 November 2001. <https://e-qanun.az/framework/18619>

**Date of receipt of the article in the Editorial Office
(01.12.2023)**