European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com

e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2020.04.72

PEDTR 2019

18th International Scientific Conference "Problems of Enterprise Development: Theory and Practice"

DETERMINATION OF TERRITORIAL JURISDICTION IN THE INVESTIGATION OF CRIMES COMMITTED IN CYBERSPACE

T. Kalenteva (a)*
*Corresponding author

(a) Samara State University of Economics, 443090, Soviet Army Str., 141, Samara, Russia, advok_tak@mail.ru

Abstract

The development of information technologies is consistently included in all branches of Russian law. The widespread adoption of digital technologies in the world is causing the emergence of new forms of crime. Information relations develop quickly and become the object of encroachment by criminals. This has led to a widespread form of crime, such as cybercrime. At the same time, the content of this term includes not only computer crimes, but also other crimes committed on the Internet. The principle of territoriality is one of the system-forming principles of criminal proceedings. However, the increase in the number of crimes committed through the use of digital technologies makes us think about the issues of determining the territorial jurisdiction in a situation where it is impossible to determine the territory where the crime was committed. The issues of determining the jurisdiction that applies to crimes committed in cyberspace, as well as determining the territorial jurisdiction and jurisdiction of these crimes, are considered. It is concluded that when determining the place of commission of a crime in cyberspace, it is advisable to proceed from the place where the victim, not the perpetrator, lives. This approach will also solve the problem of transferring materials from one territorial authority to another in search of the crime scene, will allow you to quickly and timely initiate criminal cases and start an investigation.

Keywords: Criminal procedure, preliminary investigation, cyberspace, investigation, jurisdiction, place of crime.

https://doi.org/10.15405/epsbs.2020.04.72
Corresponding Author: T. Kalenteva
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

The formation of the information society in Russia is becoming the cause of new forms of crime. Information relations develop quickly and become the object of encroachment by criminals. This has led to a widespread form of crime, such as cybercrime. Cybercrime is a complex and multifaceted phenomenon. The current criminal law does not provide a legal definition of crime in cyberspace, so you should refer to the literature. In general, cybercrimes are distinguished from other types of crimes by specific features of the objective side (object, means, place of commission).

The term "cybercrime" is controversial in the literature. This term is often equated with computer crime, but these are different concepts. In Russian criminal law, the term "computer crime" is used. This term covers all crimes included in Chapter 28 of the Criminal code of the Russian Federation from 13.06.1996 N 63-FZ "Crimes in the field of computer information" (articles 272 to 274.1). However, all these compounds consider computer information and computer programs as an object of influence or as a means of influence (Korobeev, Dremlyuga, & Kuchina, 2019). We believe that the concept of "cybercrime" can be considered both in a narrow and broad sense. In a narrow sense, these are exclusively computer crimes. That is, crimes that infringe on the safe functioning of computers and computer networks and the information located there. Cybercrime in the broad sense of the term is all crimes committed using various digital technologies.

Characteristic features of cybercrime are:

- Variety of objects of encroachment;
- The object and means of committing such crimes - information;
- The crime scene is cyberspace.

The Budapest Convention of the Council of Europe on cybercrime of 2001, classifies 4 groups of criminal acts as cybercrimes:

1) Crimes aimed at changing and deleting data stored in information networks;

2) Crimes against the availability, integrity and confidentiality of computer data, which include such crimes as unauthorized access to computer data, illegal interception of computer data, impact on information, as well as impact on the functioning of computer systems);

3) Crimes that involve the use of computer technology;

4) Crimes related to violation of related and copyright rights (Bajovic, 2017).

In accordance with the current criminal procedure legislation, a preliminary investigation is carried out at the place where the crime was committed. If the crime was started in one place and ended in another, the criminal case is investigated at the place where the crime was committed. When investigating crimes committed in cyberspace, it is not always possible to determine the place of the crime and the location of the offender. In addition, it is very rare to determine the time of the end of the crime, especially to establish the place where the crime was completed.

2. Problem Statement

In the context of modern digitalization of society, the law enforcement system must also change. More and more often there are issues related to the revision of issues related to the definition of territorial

https://doi.org/10.15405/epsbs.2020.04.72
Corresponding Author: T. Kalenteva
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

jurisdiction and jurisdiction. The modern criminal keeps up with the times (Ivantsov, Sidorenko, Spasennikov, Berezkin, & Sukhodolov, 2019). He became more sophisticated in choosing ways to commit a crime. If possible, it chooses a non-contact method of committing the crime, and the place of committing the crime is cyberspace. Some criminals can be tracked using IP address detection. However, the proportion of offenders successfully hide their actual location. For this purpose, there are anonymizers, open proxy servers, programs with end-to-end double encryption, etc. Under these conditions, it is not possible to determine the location of the person committing the crime, as well as to determine exactly where it was committed (Maillart, 2019). The question arises: which territorial investigation body should initiate a criminal case and where should the preliminary investigation be carried out? As a result, the question arises about the need to revise the modern approach to the definition of territorial jurisdiction.

3. Research Questions

The subject of the study is the issues of determining the place of Commission of crimes, if they are committed in cyberspace. We investigate cases where there is no technical ability to determine the location of the computer from which the offender was connected to the network, as well as the location of the offender at the time of the crime. The issue of changing the existing approach to the modern definition of territorial jurisdiction is considered.

4. Purpose of the Study

In the framework of this study, the author aims to study issues related to modern views on the institution of territorial investigation as a fundamental position of preliminary investigation in the conditions of digitalization of society, as well as to develop proposals aimed at solving the existing problem. Various approaches to the issue of determining territorial jurisdiction in the world criminal procedure practice as well as in the domestic one are investigated. Various options for solving this problem are analyzed, and an attempt is made to develop an author's approach to solving it.

5. Research Methods

In general, this study was conducted using the dialectical method of cognition. Along with the dialectical method of cognition, general scientific methods were used: the method of analysis and synthesis, and the method of formal logic. Special methods of cognition were also used: logical, comparative, and systemic. As private methods, comparative legal and formal legal methods, the method of processing and actual study of the material, and the method of interpretation of law were used.

6. Findings

Determining the location of a crime in cyberspace is key, since the speed and usefulness of the investigation depends on its correct and timely establishment. This will allow you to collect and consolidate evidence in a criminal case as soon as possible, which, in turn, will allow you to bring the person responsible

https://doi.org/10.15405/epsbs.2020.04.72
Corresponding Author: T. Kalenteva
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

for the crime to criminal responsibility within a reasonable time and make a legal, reasonable and fair decision.

According to Odintsov and Vashchenko (2016), cyberspace includes a social aspect and a spatial aspect. They propose to consider cyberspace in the broad sense of the word as an imaginary environment in which interaction takes place using computer technologies and which is perceived by encoding visual and audio signals. Cyberspace can appear in any information and telecommunications network. For example, within the Internet, you can talk about the Internet space. Therefore, the Internet is not cyberspace itself, but only a condition in which it can exist (Prostoserdov, 2016). According to Deineko (2018), cyberspace is made up of the Internet, FTP networks, and peer-to-peer TOR networks.

For legal analysis of cyberspace, it is preferable to follow the Model law on cybercrime of the International Telecommunication Union. This law defines cyberspace as a physical and non-physical space created and / or formed as follows: computers, computer systems, computer networks, their computer programs, data, and users.

If cyberspace is considered as a crime scene, then the question arises how to determine the rules of operation of the criminal law on the territory. Cybercrimes often go beyond the usual structures, do not have state borders (transnational) (Velasco, 2015; Maillart, 2019; Parhomenko & Evdokimov, 2015). In itself, the place where the crime was committed is the territory where the criminal act was initiated or completed, or where socially dangerous consequences occurred.

Ishin (2017) explores cyberspace within the framework of information law. It treats cyberspace as:

1) Combining computer networks and information resources that do not have a specific owner;

2) A single space of human communication;

3) A decentralized space that no state fully owns or manages;

4) A heterogeneous space where everyone can use the information resources of all mankind at their own discretion.

Regarding cyberspace, it is noted that it is hypothetically possible to localize a legal fact on the Internet. For this purpose, information about the location of the server, the domain area, the location of the computer on the nationality of the user, a private person, on national jurisdiction-the organization, etc. (Ishin, 2017). To determine the location of the crime in the network, it is necessary to consider the legal regime of this network. The most common network used by criminals to commit crimes is the Internet, so we will analyze the legal regime on its example.

Some researchers propose to consider the legal regime of the Internet by analogy with international and open spaces. Some attribute the Internet to international spaces such as Antarctica, space, and the high seas, and believe that they are not subject to national sovereignty. Volevodz (2002) proposes to refer the Internet to territories with a mixed legal regime (territorial waters of coastal States, exclusive economic zones, continental shelf, rivers). It seems to us that cyberspace has specific properties and cannot be put on a par with the listed territories.

Can we talk about extending the state's sovereignty to the national segment on the Internet? The national segment of the Russian Federation in cyberspace (Runet) is represented by the domains: "ru", "RF", "su". It turns out that the criminal law of the Russian Federation should apply to sites with these domains. However, there are international domains in the network that do not belong to a particular state.

https://doi.org/10.15405/epsbs.2020.04.72
Corresponding Author: T. Kalenteva
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

Information can be physically located on the site of a domain that belongs to Runet, but stored on a server of another state. In these cases, it is not possible to determine which state's sovereignty extends to the information. In addition, due to the rapid development of information technologies, other domains can be created, which can make it difficult to classify the site as a Runet.

The principle of national jurisdiction is defined in the CIS model law «On the basics of Internet regulation» (application to the resolution of the IPA CIS dated May 16, 2011 No. 36-9). In accordance with article 11 of this law, all actions that have legal significance and are carried out using a computer network (Internet) are considered committed on the territory of the state if the specified action meets one of the following criteria:

- The person at the time of this action was actually located on the territory of this state;
- The commission of this action caused damage in the territory of this state;
- This action was performed using a technical device that was physically located on the territory of this state at the time of such action (cis model law «on the basics of internet regulation» (application to the resolution of the IPA CIS dated May 16, 2011 No. 36-9)). At the same time, disputed cases of territorial jurisdiction are regulated by international agreements.

The principle of national jurisdiction enshrined in the Model law of the CIS is consistent with the principles of determining the place of Commission of a crime under the Criminal code of the Russian Federation from 13.06.1996 N 63-FZ: territorial, real, universal principles and the principle of citizenship. The researchers suggest using these principles taking into account such a feature of cybercrime as cross-border activity. The content of the principles directly depends on the structure of the crime. Crimes with material content fall under the jurisdiction of the state that was harmed by this crime. Formal and truncated compositions are subject to the criminal law of the country where the device is located, which is the method of committing the crime. This approach has a great practical orientation, but is not ideal, since many elements of crime cannot be attributed to any one specific type (for example, if the crime leads to the occurrence of various consequences). An act may also be qualified by a combination of crimes.

The position on this issue has not been formulated by the higher courts. Let's turn to the judicial practice of one of the most common crimes – fraud in the field of computer information (article 159. 6 of the Criminal Code of the Russian Federation from 13.06.1996 N 63-FZ).The main issues related to the application of this article are covered in the resolution of the Plenum of the Supreme Court of the Russian Federation No. 48 dated 30.11.2017 "On judicial practice in cases of fraud, embezzlement and embezzlement". However, the mentioned act does not address the issues of determining the place of committing fraud in the field of computer information, although this issue is directly related to determining the territorial jurisdiction of crimes of this type. If we analyze the draft Resolution, we can understand that the Plenum of the armed forces of the Russian Federation has two positions on this issue, which are formulated on the example of non-cash funds. If the subject of fraud is non-cash funds, the place of commission of the crime on the one hand will be the actual location of the guilty person at the time of the action, and on the other hand-the location of the Bank (its branch) or other organization in which the owner of the funds opened a Bank account or kept records of electronic money without opening an account. As we can see, the issue we are considering is not reflected in the published Decision, but remains at the development stage.

https://doi.org/10.15405/epsbs.2020.04.72
Corresponding Author: T. Kalenteva
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

It seems to us that the place where "digital theft" was committed should be considered the place where it was finished – where the victim was harmed. Such a place is considered by the courts to be the place of opening the victim's account or the place of maintaining his electronic wallet. This position of the courts takes into account the interests of persons affected by digital theft. Let us turn to the appeal decision of the Lipetsk regional court of 26.12.2017 in the case N 22-1739/2017, which illustrates the court's position.

A case involving the theft of non-cash, was sent to the court of first instance (Federal court of the Soviet district of the city of Lipetsk), depending on the crime (find the Bank branches where open the account and where transferred funds after the Commission of the theft). The court of appeal overturned the decision to send the criminal case under jurisdiction to the specified court, based on where the money was originally stored, and where the objective side of the act was performed (theft of money). The court of appeal in making the relevant decision was guided by part 2 of article 32 Code of criminal procedure of the Russian Federation: if the crime was started «in a place within the jurisdiction of one court and completed in a place subject to the jurisdiction of another court, the given criminal case shall be tried by the court at the place where the crime» (Criminal procedure code of the Russian Federation of 18.12.2001 N 174-FZ (ed. of 27.12.2019)). In this case, in the sense of section 5 of the Resolution Of The Plenum Of The Supreme Court Of The Russian Federation no. 48 of the theft of non-cash is over "from the moment of withdrawal of funds from the Bank account of their owner or electronic funds, as a result of which the owner of these funds has suffered damage" (Resolution of the Plenum of the Supreme Court of the Russian Federation No. 48 dated 30.11.2017 "On judicial practice in cases of fraud, embezzlement and embezzlement")

Quite a confusing way to solve the problem. As a result, the place of the crime was equated to the place of the end of the crime, and this place became the Bank where the victim's money was originally stored.

In the Oktyabrsky district of Samara, a criminal case was opened on the fact of embezzlement of funds from an electronic wallet P. - Criminal case No. 11701360001014328 (Police Department for the Industrial District of Samara, 2019). These funds were withdrawn to the Bank's current account, and at a later period they were paid for a purchase in the online store. Investigative actions and operational search measures to establish the IP address of the computer and its location at the time of the crime did not yield results. There was a question of determining the territorial jurisdiction of this criminal case. Statement P. filed at the place of his actual residence. During the preliminary investigation, it was found that P. was registered at an address located in the Industrial district of the city of Samara. The materials of the criminal case were transferred to the Prosecutor to resolve the issue of transferring the criminal case in accordance with the rules that define the rules for determining the territorial jurisdiction. The Prosecutor sent the criminal case for further investigation to the police Department serving the Industrial district of the city of Samara.

Investigative practice in such cases in the city of Samara is as follows: a statement about a crime received by law enforcement agencies is checked for registration of the applicant at the place of residence. If it was not possible to determine the location of the computer from which the access to the network was carried out, or if it was not possible to determine the place where the stolen funds were cashed, and there

https://doi.org/10.15405/epsbs.2020.04.72
Corresponding Author: T. Kalenteva
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

are no witnesses to the crime, then a criminal case is initiated at the place of registration of the applicant (victim).

We looked at a situation where non-cash funds were the subject of digital theft. In this case, the place of the crime was determined based on the place of storage of these funds. At the same time, the crime was not committed on the Internet. The question remains how to determine the place of Commission of a crime committed directly on the Internet, and the territorial jurisdiction of such a crime. For example, if there was a crime such as phishing. Phishing (eng. "phishing", distorted "fishing" – "fishing") – mass mailing of emails or messages in order to lure the user to web sites that look very similar to the usual web sites of various firms and banks, but are controlled by fraudsters(Marcum & Higgins, 2019). This act is classified as a type of fraud in the field of computer information.

As we have already found out, the trend of determining the place of Commission of cybercrimes is related to the place of the end of the crime in cyberspace. Due to the fact that the result of phishing is not the taking of someone else's property, the time of the end of such a crime cannot be determined by the General rule. Phishing is considered to be over when performing actions aimed at mass mailing of e-mails or emails. These actions are performed using a computer or other device via the Internet. When committing the specified crime, it will indicate the IP address to which the address of the suspect's residence is assigned under the agreement between the user and the provider, if the suspect did not take measures to replace the IP address. The technology of spoofing the real IP address of the criminal's computer involves, most often, the use of IP addresses issued for spoofing by foreign providers, resulting in the impression that the criminal is abroad. Spoofing an IP address is only one of the problems of determining the IP address of a criminal's computer. An incorrect definition of the IP address affects the erroneous determination of the place where the cybercrime was committed (in d. SL. phishing), and therefore the territorial jurisdiction of this crime.

In our view, it is appropriate to determine the location of a crime in cyberspace based on where the victim, not the perpetrator, lives. If we take into account the purpose of criminal proceedings, we must remember that the first task is to protect the rights and legitimate interests of victims of crimes. However, this approach will be optimal only at the stage of initiating a criminal case. The investigator will be able to make a decision about initiating a criminal case without sending materials on the investigation. This option will also solve the problem of transferring materials from one territorial authority to another in search of the crime scene, will allow you to quickly and timely initiate criminal cases and start an investigation. This approach will minimize efforts in determining the location of cybercrime.

7. Conclusion

When a crime is committed in cyberspace, it is most logical to link the operation of the criminal law in cyberspace either to the place of the end of the crime or to the place of residence of the victim. In this case, it is not necessary to take into account the location of the offender, the territory where the damage was caused, and the location of the technical device that is the method of committing the crime. As an attempt to develop a uniform approach to this problem, it is proposed to legislate the definition of cyberspace and the procedure for determining the place of crime in it.

The territorial jurisdiction of cybercrimes should be determined taking into account the place of origin and the place of termination of the act. At the same time, these categories should be fixed in The

Resolution of the Plenum of the Supreme Court of the Russian Federation No. 48 dated 30.11.2017 "On judicial practice in cases of fraud, misappropriation and embezzlement" for each crime committed via the Internet separately, since each individual act has its own specific characteristics. In our opinion, special attention should be paid to the place of the end of the crime. In other words, fixing the problem with the definition of territorial jurisdiction crimes in cyberspace is only possible to achieve by gripping the end of a certain cyber crimes in the relevant act of the Plenum of the RF armed forces. We can assume that in the future this category of crimes will become the main form of crimes, so the problems we have raised cannot remain without consideration.

Acknowledgments

The author expresses great gratitude to the Samara state University of Economics for its full support and the opportunity to conduct research.

References

Appeal decision of the Lipetsk regional court of 26.12.2017 in the case N 22-1739/2017. Retrieved from https://oblsud--lpk.sudrf.ru/modules.php?name=sud_delo&srv_num=1&name_op=doc&number=30539983&delo_id=4&new=4&text_number=1&case_id=49291 Accessed: 02.11.2019.

Bajovic, V. (2017). Criminal proceedings in cyberspace: The challenge of digital era. In E. Viano (Ed.), *Cybercrime, Organized Crime, and Societal Responses* (pp. 87-101). Cham: Springer. DOI: 10.1007/978-3-319-44501-4_5.

CIS model law «On the basics of Internet regulation» (application to the resolution of the IPA CIS dated May 16, 2011 No. 36-9). Retrieved from https://www.russianlaw.net/law/general/t73/ Accessed: 08.12.2019.

Criminal code of the Russian Federation from 13.06.1996 N 63-FZ (as amended on 27.12.2019). Retrieved from http://www.consultant.ru/document/cons_doc_LAW_10699/ Accessed: 02.11.2019.

Criminal procedure code of the Russian Federation of 18.12.2001 N 174-FZ (ed. of 27.12.2019). Retrieved from http://www.consultant.ru/document/cons_doc_LAW_34481/ Accessed: 02.11.2019.

Deineko, G. (2018). Cyberspace law: Pro et contra. In M. A. Rozhkova (Ed.), *Law in the Internet: A Collection of Articles. Series 14 - Analysis of Modern Law* (pp. 246-255). Moscow: Statute.

Ishin, A. M. (2017). Internet and cybercrime: Some aspects. In O. A. Zayachkovsky (Ed.), *Modern Problems of Legal Science and Law Enforcement Practice* (pp. 346-352). Kaliningrad: Baltic Federal University named after I. Kant.

Ivantsov, S. V., Sidorenko, E. L., Spasennikov, B. A., Berezkin, Y. M., & Sukhodolov, Y. A. (2019). Cryptocurrency-related crimes: Key criminological trends. *Russian Journal of Criminology, 13*(1), 85–93. DOI: 10.17150/2500-4255.2019.13(1).85- 93 [in Rus.].

Korobeev, A. I., Dremlyuga, R. I., & Kuchina, Y. O. (2019). Cybercrimes in the Russian Federation: Criminological and criminal law analysis of the situation. *Russian Journal of Criminology, 13*(3), 416–425. DOI: 10.17150/2500-4255.2019.13(3).416-425 [in Rus.].

Maillart, J. B. (2019). The limits of subjective territorial jurisdiction in the context of cybercrime. *ERA Forum, 19,* 375. DOI: 10.1007/s12027-018-0527-2

Marcum, C. D., & Higgins, G. E. (2019). Cybercrime. In M. D. Krohn, N. Hendrix, G. P. Hall, A. J. Lizotte (Eds.), *Handbook on Crime and Deviance. Handbooks of Sociology and Social Research* (pp. 459-479). Cham: Springer.

Odintsov, S. A., & Vashchenko, A. V. (2016). The development of the theory of the informational society and cyberspace. *Polythematic Online Electronic Scientific Journal of the Kuban State Agrarian University, 121*(07), 1850-1863.

Parhomenko, S. V., & Evdokimov, K. N. (2015). Prevention of cybercrime in the Russian Federation: An integrative and comprehensive approaches. *Criminology Journal of Baikal National University of Economics and Law, 9*(2), 265–276. DOI: 10.17150/1996-7756.2015.9(2).265- 276 [in Rus.].

Police Department for the Industrial District of Samara (2019). *Criminal case No. 11701360001014328.* Samara: Archive of the Police Department for the Industrial District of Samara.

Prostoserdov, M. A. (2016). *Economic crimes committed in cyberspace and measures to counter them: Dissertation for the degree of candidate of legal sciences*. Moscow: Russian State University of Justice.

Resolution of the Plenum of the Supreme Court of the Russian Federation No. 48 dated 30.11.2017 "On judicial practice in cases of fraud, misappropriation and embezzlement". Retrieved from https://legalacts.ru/sud/postanovlenie-plenuma-verkhovnogo-suda-rf-ot-30112017-n-48/ Accessed: 11.11.2019.

Velasco, C. (2015). Cybercrime jurisdiction: Past, present and future. *ERA Forum, 16*, 331–347. DOI: 10.1007/s12027-015-0379-y

Volevodz, A. G. (2002). *Countering computer crimes: Legal framework for international cooperation.* Moscow: Yurlitinform.