*Advances in Economics, Business and Management Research, volume 171*
**Proceedings of the 1st International Scientific Conference "Legal Regulation of the Digital Economy and Digital Relations: Problems and Prospects of Development" (LARDER 2020)**

# Problems of Proof of Illegal Use of Copyright for Computer Programs

Vladimir Ivshin[1,*] Artem Shmarev[1] Sergey Starodumov[1]

[1]*Udmurt State University, Izhevsk 426034, Russian Federation*
[*]*Corresponding author. Email: old21@mail.ru*

**ABSTRACT**
The article deals with the problem of criminal law evaluation of the use of access to a protected copyright object imitating a computer program access key. An analysis of the mechanism of the commission of the crime and the problems of proof arising in such criminal cases is provided. These circumstances are due to the development of software used for computer operation. The need to protect the legitimate interests of their rights holders, that is, the fight against "piracy," becomes particularly urgent. First of all, these rights are regulated by copyright, but the criminal law does not ignore them. In the investigation of such criminal cases, there are difficulties in identifying copyright objects. As a method of accessing a protected copyright object, a computer program access key simulation is used. Such a method is called "crack." Can such imitation be referred to as an object of copyright when the right holder sets the access key to the computer program as an independent object of sale. The study is devoted to refuting the argument about the possibility of identifying the simulation of access to the computer program and the access key itself as the use of a single copyright object.
***Keywords:*** *Cybercrimes, harmful software, information security, malware, computer virus.*

## 1. INTRODUCTION

Relations in the scope of intellectual property are currently developing rapidly. The first among the objects of intellectual rights are those that ensure the use of computers – programs for computers, and computer information that forms unique content on the Internet, to which the copyright holder provides access to users [1].

The legislator, recognizing the importance of legal relations in the field of intellectual property, protects their participants, including criminal legal remedies. The qualitatively changed actual relations of participants in the copyright market have determined new ways of interaction between their subjects, which is directly reflected in the methods of committing crimes in the field of copyright.

The development of the Internet has determined new possibilities for transferring legal copyright objects and additional ways of protecting these objects by their copyright holders. methods of copyright violation, based on physical copying of these objects to material media - disks and flash drives, go into the past. In fact, any computer program, film or other object can be downloaded from the Internet using cloud-based information stores and related methods of transmitting it. Under these conditions, copyright holders began to use additional ways to protect their products [2].

Such methods include the use of license keys. This key allows only the owner of the key to access the copyright object. This scheme of protection of the copyright object complicates or effectively eliminates the possibility of uncontrolled copying of such objects in addition to the will of the copyright holder. On the other hand, the license key allows you to provide a multi-user mode of operation in the program. For example, one program is installed from one tangible media to several computers, and it is accessed by as many users as possible to connect a license key. In this case, the user group is able to work in the same program database together.

Thus, the license key acts as a hardware means of protecting the copyright object, that is, a means of protection that the copyright holder himself has embedded in the protected object. A form of implementing license keys is the use of it on a material medium - a flash drive or in the form of a unique digital code.

Our research objective is to develop recommendations aimed at the law enforcement officer and aimed at improving the practice of investigating criminal cases of copyright offences in the field of computer information. A related goal is analyzation of the criminal qualification of the use of malicious computer programs in the form of an emulator of electronic remedies for crimes under article 146 of the Criminal Code of the Russian Federation.

## 2. MAIN RESULTS

The criminal legal problem is created by the marketing policy of implementing programs for computers by their rights holders in combination with the emerging ways of violating their copyright. Article 146 of the RF Criminal Code provides for two forms of implementa-

tion of the objective side. On the one hand, part 1 ar.146 of the RF Criminal Code involves the appropriation of authorship, and on the other hand, part 2 ar.146 of the RF Criminal Code provides for the illegal use of copyright objects, including the acquisition, storage and transportation of counterfeit copies. A constructive sign of the corpus delicti is the causing of major damage to the copyright holder. The purpose of committing unlawful acts provided for in parts 1 and 2 of article 146 of the Criminal Code of the Russian Federation differs significantly, in connection with which we believe it necessary to dwell on the content of the corpus delicti providing for the illegal use of copyright objects.

Thence, some rights holders, realizing their product, that is, a program for computers, take a differentiated approach to generating the price of the final product purchased by the user. For example, the cost of the software product itself, that is, a copyright object with the right of access to it by one user may not fall under a large size. On the other hand, the cost of purchasing a multi-user mode of access to the same program will already fall under the large size. This differentiation may be due to the desire to interest large enterprises or "businesses" in the purchase of a software product, for its use in the activities of the company everywhere.

At the same time, the most common method of providing access to the multi-user mode is carried out using the license key used in conjunction with the main program provided by the copyright holder.

Currently, offenders have learned to overcome this way of protecting software products. One such method is the use of license key emulators provided by the copyright holder. These emulators allow you to use the computer program in the absence of a license key. Such an emulator, or as it is called "crack," has the form of a file that simulates the operation of a license key, both in the form of a USB key and in the form of a digital code. This way of overcoming hardware protection of computer programs can create certain problems of criminal legal qualification of such illegal actions [3].

Thence, on May 07, 2019, the Glazovsky interdistrict investigation department of the Investigative Department of the Investigative Committee of the Russian Federation for UR opened a criminal case on the grounds of the corpus delicti under Part 3 of Article 166 of the Criminal Code of the Russian Federation against an unidentified person from among the employees of one company. From the prosecution it followed that the copyright holder suffered particularly large damage for 3169,200 rubles by using illegal programs on five computers of the company.

During the appointed computer expertise, it was found that the software for computers belonging to the copyright holder was installed on the seized computers. On the equipment of the expert, the program was launched, but to continue work required the use of a license key.

On seized computers, the program was launched and worked in the absence of electronic hardware protection keys. A file was also found, when adding to the files of the computer program on the equipment of the expert, the latter began to work. At the same time, the inscription "Client license for 50 jobs" appeared. At the same time, the expert could not determine the nature of the file, the use of which made it possible to run the program for computers.

In substantiating the damage caused, the copyright holder submitted a price list containing prices for computer programs that he implements. The cost of the program depended on the number of users, increasing in proportion to the growth in the number of users. Justifying the total amount of damage caused in the amount of 3169,200 rubles, the representative of the victim indicated that the software products of the copyright holder "Client license for 50 jobs," "Client license for 500 jobs" were used on the seized computers, and their total cost is the amount of damage caused [4].

From the testimony of the system administrator who used the software product, it followed that the legal entity had previously purchased a license program for the computer of this copyright holder with access for one user. When company using the program, it was necessary to install it on 5 computers in 5 different stores of the company. But for the normal functioning of the company's activities, he needed to purchase another 4 programs for each individual computer. Instead, he downloaded several access key emulators to this program on the Internet. Then, on all five computers, he installed a previously purchased program. After that, he randomly installed previously downloaded access key emulators on all five computers in the company's stores. Only one user was required and used on each computer. It was a merchant. At the same time, the minimum cost of the program for computers, according to the price list of the distributor, was 14,000 rubles, which did not allow to qualify its illegal use as a crime due to the lack of consequences on a large damage.

In this situation, the prospect of challenging the classification of unlawful actions as a criminal offense is indicated on the basis of the absence of a large amount of damage caused to the copyright holder. According to the note to article 146 of the Criminal Code of the Russian Federation, acts are recognized as committed on a large damage if the cost of copies of works or phonograms or the cost of rights to use copyright and related rights exceeds one hundred thousand rubles, and on a very large damage - one million rubles. In accordance with the Decision of the Plenum of the Supreme Court of the Russian Federation of 26.04.2007 N 14 "On the practice of courts considering criminal cases of violation of copyright, related, invention and patent rights, as well as the illegal use of the trademark," the amount of damage caused to the copyright holder is determined regardless of the occurrence of criminal

consequences in the form of actual damage to the copyright holder. Taking into account these explanations, the question arises as to how to determine the value of the copyright object, under the conditions set forth in these circumstances [5].

The copyright holder believes that the damage is determined based on the actually discovered access to the program in multi-user mode. The offender believes that he caused damage in the amount of the cost of the program in the minimum amount.

We believe that a formal approach to determining the amount of damage is unacceptable under the circumstances. It is also unacceptable to mix the damage caused by criminal and civil relations.

In these circumstances, attention should be drawn to the fact that the multi-user mode of access to the computer program was obtained by the offender using the emulator key in the computer program belonging to the copyright holder. These circumstances are confirmed by the conclusion of an expert on the results of a study of system blocks seized from the offender.

Thus, according to the mechanism for committing the crime, the offender used some means - an access key emulator - to gain access to the protected copyright object. At the same time, this tool made it possible to use the copyright holder's program in a more expensive version.

The criminal legal assessment of the mechanism for committing copyright infringement directly affects the determination of damage from this crime. Very important in this case is a means of overcoming the hardware protection of the copyright object - the computer program. If the damage caused by these crimes is considered, then it is determined by the value of the copyright object. At the same time, it becomes difficult to determine the value of the copyright object, since there is no certainty in the issue of determining its size.

One can specify the following example for comparison. The cost of most computer programs itself falls under the large size, such cases include the cost of well-known design programs, text editors, and so on. In case of violation of the rights of their owner, the actions of the offender are automatically subject to criminal liability under article 146 of the Criminal Code of the Russian Federation. In the situation described above, the potential amount of damage determined by the copyright holder was made up of the cost of the program and the cost of the separately purchased license key. Thus, if in itself the license key belonging to the copyright holder was not used, but a similar program was used, then how lawful it is to include its cost to the general detriment.

Since the object of the crime under article 146 of the Criminal Code of the Russian Federation is copyright, the damage caused by this crime must be caused by copyright. In the situation described in the article, the offender was intent on using a computer program in violation of the rights of its owner. The offender lacks the purpose and intent to use the license key as an independent copyright object. The license key itself is not of commercial or industrial interest.

Since the intent of the offender is aimed at the unlawful use of the copyright holder's program for its intended purpose, he needs to overcome its remedies. For this, the offender uses a means similar to the hardware key of the defense, which is not the product of the copyright holder.

This feature of this type of crime is of great importance. It would seem that if this method of committing these crimes were not taken into account, this would entail a violation of the principle of fairness both in determining the damage caused by the crime and in determining the balance of responsibility for the offense committed.

Moreover, the method of committing these crimes, provided for in both part 2 and part 3 of article 146 of the Criminal Code of the Russian Federation, described above, is more similar to the signs of a crime under article 273 of the Criminal Code of the Russian Federation. The use of the access key to the copyright holder's program, which was not created by this copyright holder or not specifically provided for by the copyright holder, more indicates the intruder's desire to gain access to the program's computer information in order to use its functionality. Thus, these acts of the offender resemble the use of computer programs or other computer information, obviously intended to neutralize the means of protecting computer information.

At the same time, researchers in this area do not keep pace with changing social relations. Therefore, to a greater extent, the scientific approach is several years behind. As a rule, the approach to understanding the expression of the objective side of article 273 of the Criminal Code of the Russian Federation remains at the level of viruses and "infection" of computers or networks [6]. At the same time, researchers bypass the forms of expression of criminal actions in reality, as well as their characteristics.

An example similar to the one demonstrated by the authors above is partly described in the article by Stepanov-Egiyants [7]. The jurisprudence he used refers to the verdict of the Soviet District Court of Tomsk of 14 October 2010 [15]. According to this example, the files "acadfix.reg," "license.lic," "licpath.lic" are not themselves programs, but only are already modified files of the program "AutodeskAutoCAD 2004," when replacing them (similar files contained in the program directory) or adding them in some cases with these modified files, the program installed in addition to the will of the copyright holder becomes functional.

Another similar example is contained in the study of Evdokimov, in which he used as an example the verdict of the Kuzminsky District Court of Moscow in 2013 in criminal case No. 1-968/13 [8]. However, Evdokimov

believes that under the circumstances set forth, the actions of the perpetrator are additionally subject to qualification under article 272 of the Criminal Code of the Russian Federation.

Stepanov-Yegiyants made a reasonable conclusion that these actions fall under the liability provided for in Article 273 of the Criminal Code of the Russian Federation.

A similar position is consistently enshrined in the comments on the criminal code edited by Lebedev. According to this position, the most common types of malware are computer viruses, worms, Trojan horses, scanner programs, *electronic protection emulators* (highlighted by the author, approx.), computer information flow control programs [9, 10].

This position is reflected, among other things, in the scientific and practical manual edited by Galakhova [11]. The approach reflected in this manual to the content of the concept of "malware" is quite consistent with the position of the authors. In this case, the essential signs of this "subject" of the crime are correctly reflected, to which:

1) The performance of undesirable functions not authorized by the copyright holder. The unwanted function also includes the failure of the information protection system;

2) Program compilation, that's means a form of program expression in electronic form with the potential to perform malicious functions.

However, errors in the criminal law assessment of the commission of unlawful acts also entail the issuance of judicial decisions with erroneous legal qualifications, which are absolutely opposite to the examples given above.

According to our example, the magistrate issued a decision to dismiss the criminal case with the imposition of a criminal law measure in the form of a court fine [12].

According to the verdict of the Shcherbinsky District Court of Moscow of October 29, 2018, upheld by the appeal decision of the Moscow City Court of March 19, 2019, a citizen of S.A., with a similar method of committing a crime, was found guilty only of committing a crime under Part 2 of Article 166 of the Criminal Code of the Russian Federation [14].

On the other hand, the decision of the Moscow City Court of September 18, 2017, which refused to transfer the supervisory complaint of the convicted K. about the revision of the verdict of the Nagatinsky District Court of Moscow of June 28, 2006, qualified similar actions both under article 146 of the Criminal Code of the Russian Federation and under article 273 of the Criminal Code of the Russian Federation [13].

These examples point to the lack of unity of jurisprudence in the consideration of criminal cases, taking into account the circumstances indicated. There can be many reasons for such contradictions, including the absence of appropriate explanations from the plenum of the Supreme Court.

## 3. DISCUSSIONS

Thus, the following problems that arise in the investigation of this category of criminal cases can be distinguished:

1) The use by offenders of computer information that allows circumventing the hardware protection of programs for computers as copyright objects;

2) Mistakes of qualification as a single crime of compositions in which copyright infringement is committed using malicious computer programs (another computer information);

3) Incorrect methodology for estimating the amount of damage caused to the copyright holder in cases where the amount of damage is determined by the cost of hardware protection (licenses), and not the cost of the copyright object to which the offender improperly accesses.

Therefore, in these circumstances, the facts related to the establishment of a method of access to protected copyright objects are to be proved. These facts must be clarified by a forensic examination. At the same time, the expert's permission should be asked about the nature of files or programs, taking into account which copyright objects are accessed in the absence of a license.

Based on the position stated by us, we consider the most reasonable and fair legal qualification of the use of electronic means of protection by offenders of emulators, and in the common people "mallard," as subject to article 273 of the Criminal Code of the Russian Federation, that is, the use of computer programs or other computer information deliberately intended for unauthorized destruction, blocking, modification, copying computer information or neutralizing means of protecting computer information.

With this in mind, it is unacceptable to identify the amount of damage caused, within the framework of article 246 of the Criminal Code of the Russian Federation, as a result of the price of a license for the program, and not the cost of the program itself, as an object of copyright.

## 4. CONCLUSIONS

All in all, in view of the contradictory judicial practice, these positions should be fixed in the Decision of the Plenum of the Supreme Court of the Russian Federation of 26.04.2007 N 14 "On the practice of courts considering criminal cases of violation of copyright, related, inventive and patent rights, as well as the illegal use of the trademark."

They can be formulated in a separate paragraph, as follows: when a person used malicious software, such

as a computer virus, worm, trojan horse, scanner program, electronic security emulator, computer information flow control program, in the commission of offences under articles 146, 147 and 180, The offence should be classified as a set of offences under article 146, article 147 or 180, and Depending on the circumstances of the particular case, in accordance with article 273 of the Criminal Code of the Russian Federation.

## REFERENCES

[1] D. A. Lipinsky, A. A. Musatkina, Social danger of offence in the scientific and legislative definitions in Russia and other countries, Journal of Advanced Research in Law and Economics 8(5) (2018) 1549-1555.

[2] B. Shakya, T. He, H. Salmani, D. Forte, S. Bhunia, M. Tehranipoor, Benchmarking of hardware Trojans and maliciously affected circuits, Journal of Hardware and Systems 1(1) (2017) 85-102. DOI: https://doi.org/10.1007/s41635-017-0001-6

[3] D.A. Lipinsky, A.A. Musatkina, The characteristic of social danger of offence in scientific and legislative definitions in the member countries of the commonwealth of independent states and European countries, Mediterranean Journal of Social Sciences 6(3) (2015) 613-616.
DOI: https://doi.org/10.5901/mjss.2015.v6n3p613

[4] R. Buchan, N. Tsagourias, Cyber War and International Law, Journal of Conflict & Security Law 17(2) (2012) 183-186. DOI: https://doi.org/10.1093/jcsl/krs016

[5] K. Barker, Cyber Criminals on Trial, International Journal of Law and Information Technology 20(3) (2012) 242-245. DOI: https://doi.org/10.1093/ijlit/eas010

[6] N.A. Golovanova, A.A. Gravina, O.A. Zajcev, Ugolovno-yurisdikcionnaya deyatel'nost' v usloviyakh tcifrovizatsii: monografiya, Kontrakt, 2019, 212 p.

[7] V.G. Stepanov-Egiyants, Otvetstvennost za prestupleniya protiv kompyuternoy informatsii po ugolovnomu zakonodatelstvu Rossiyskoy Federatsii, Statut, 2016, 190 p.

[8] K. N. Evdokimov, N. N. Taskaev, Problems of qualifying crimes under Article 273 of the Criminal Code of the Russian Federation at the stage of initiating criminal proceedings, Russian Journal of Criminology 12(4) (2018) 590-600. DOI: https://doi.org/10.17150/2500-4255.2018.12(4).590-600.

[9] Y.I. Antonov, V.B. Borovikov, A.V. Galachova, Ocenochnye priznaki v ugolovnom kodekse Rossiskoy Federatsii: nauchnoe i sudebnoe tolkovanie: nauchno-practicheskoe posobie, Norma, 2014, 736 p.

[10] A.V. Brilliantov, A.V. Galachova, V.A. Davydov, in: V.M. Lebedev (Eds.), Kommentarii k ugolovnomu kodeksu Rossiskoy Federatsii, Urait, 2017, 315 p.

[11] V.M. Lebedev (ed.) Kommentarii k ugolovnomu kodeksu Rossiskoi Federacii. M.: Urait, 2018, 687 p.

[12] Postanovlenie mirovogo sudyi sudebnogo uchastka No. 2 g. Glazova UR ot 17 octiabra 2019 g. http://glazmir2.udm.msudrf.ru Accessed on 04 Aug 2020.

[13] Postanovlenie Moskovskogo gorodskogo suda ot 18.09.2017 N 4y-5272/2017. http://www.consultant.ru/ Accessed on 10 Aug 2020.

[14] Apelyacionnoe opredeleniye Moskovskogo gorodskogo suda ot 19.03.2019 http://www.consultant.ru/ Accessed on 24 Aug 2020.

[15] Prigovor Sovetskogo rayonnogo suda g. Tomska ot 14.10.2010. https://sovetsky--tms.sudrf.ru. Accessed on 04 Aug 2020.