RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
AUGUST 2019

DOI:10.5281/zenodo.3386118

Particularities of the Forensic Investigation of Software Piracy and Online Piracy

Adrian Cristian Moise

Spiru Haret University of Bucharest, Bucharest, Romania adriancristian.moise@gmail.com

ABSTRACT: Starting from the analysis of the Law no 8/1996 on copyright and related rights in Romania, and continuing with the analysis of the main provisions of the European Union Directive 2001/29/EC on copyright and related rights in the information society and the European Union Directive 2009/24 / EC on the legal protection of computer programs, the article presents and analyzes aspects of the criminal investigation of software piracy and online piracy. The article analyzes both some of the criminal investigation acts commonly used in software piracy such as technical-scientific findings and forensic expertise of copyrighted software or related rights, and some methodological issues related to forensic investigation of software piracy and online piracy.

KEYWORDS: copyrights, forensic investigation, online piracy, software piracy

Introduction

Piracy was defined as "the unauthorized copying of the work protected by copyright or related rights, for commercial or non-commercial purposes as well as the unauthorized sale of the copied work, activity carried out by a third party, without the consent or authorization of the right holders" (Pantea 2016, 260).

Some of the areas most affected by the phenomenon of piracy are software-related, including operating systems, utility programs, but also the one related to the online domain, including illegally downloading or uploading software on the Internet, illegally displaying some works on some web pages, online games, etc.

In Romania, the protection of computer programs is governed by Law no 8/1996 on copyright and related rights. The offenses related to the protection of computer programs are provided by Law no 8/1996 in Article 194 (making the products available, without right, of the products having related rights or sui generis rights through the Internet or other computer networks), Article 195 (unauthorized reproduction on computer software systems), Article 198 (illegal use of access control devices, whether original or pirate), Article 199 (possession and illegal use of devices to neutralize technical protection measures).

The most common forms of piracy are as follows: software piracy and online piracy

According to the provisions of Art.195 of Law no 8/1996, the notion of *software piracy* consists in unauthorized reproduction of software in any of the following ways (Vasiu and Vasiu 2011, 270): *installation*, which refers to the configuration of a software in accordance with the requirements of the system; *storage*, which represents the action of preserving data and computer programs on a specific computer data storage medium; *running* or *execution*, which refers to the action of executing or running the instruction sequences of a software; *display* which refers to the presentation of the information in a form readable to the user, which can be modified to its action or the computer system; *transmission in the internal network*, representing the transmission of computer data from one digital location to another.

The notion of *online piracy* consists of computer programs that are uploaded to different websites or other computer networks so that they can be accessed by persons who are not authorized to use them. In most cases, online piracy is done through peer-to-peer networks, which represent a method used, through the Internet, to share some files between multiple computer systems within the Internet network. Peer-to-peer networks are used both to share software and to share music, video, or other files (Savin 2013, 155).

Regulating the protection of computer programs at the level of the European Union

The most important legal instruments regulating software protection at European level are: Directive 2001/29/EU of the European Parliament and of the Council of 22 May 2001 on the harmonization of certain aspects of copyright and related rights in the information society and Directive 2009/24/EU of the European Parliament and of the Council of 23 April 2009 on the legal protection of computer programs.

Directive 2001/29/EU on the harmonization of certain aspects of copyright and related rights in the information society relates to the legal protection of copyright and related rights within the internal market, paying special attention to the information society. According to Article 6 paragraph 1 of the Directive, it shall be provided adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.

Also, in Article 6(2) it shall be provided adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which: are promoted, advertised; or marketed for the purpose of circumvention of; or have only a limited commercially significant purpose or use other than to circumvent; or are primarily designed, produced, adapted and performed for the purpose of enabling or facilitating the circumvention of, any effective technological measures.

Directive 2009/24/EU on the legal protection of computer programs provides that protection is applicable to any form of expression of a computer program. The notion of *computer program* includes preparatory design material. The computer program should include programs in whatever form, including those embedded in hardware. This notion also includes preparatory design works having as purpose the development of a program on condition that they allow the creation of a computer program in a later stage.

According to Article 1 paragraph 3 of the Directive 2009/24/EU, a computer program shall be protected if it is original in the sense that it is the author's own intellectual creation. No other criteria shall be applied to determine its eligibility for protection. The exclusive rights of the holder include the right to make or authorize, in accordance with Article 4: "permanent or temporary reproduction of a computer program, by any means and in any form, in part or in whole".

Major problems to be clarified in the forensic investigation of software piracy and online piracy

The major problems to be clarified regarding the forensic investigation of software piracy and online piracy refer to the following aspects:

Establishing the existence of illicit activity of software piracy or online piracy

For the purpose of investigating the criminal activity of one or more individuals, the investigators must first establish the existence of the offense related to software piracy or online piracy.

In the case of the offense under Article 194 of Law no 8/1996 on copyright and related rights, illicit activity consists of *making available to the public, including via the Internet or other computer networks, without right, of works or products carrying related rights or sui generis rights of the producers of their databases or their copies, regardless of the medium, so that the public to access them anywhere or at any time individually chosen*.

A frequent way of committing this offense is software piracy committed through the Internet, that is, the act of hosting software carrying copyright or related rights that can be accessed from different websites by any person who meets certain conditions. Another frequent way of committing the offense, stipulated by Article 194, refers to allowing people to access their own computer system through Peer-to-Peer (P2P) software that is used to share files between several computer systems linked to each other on the Internet (Moise 2011, 348). We point out that P2P is often legally used to share music, video, and other types of files and software. The most common

file sharing programs are: KaZaA, Morpheus, Gnutella, FreeNet, WinMx, iMesh. The KaZaA file-sharing program can be used to share many types of files, including images and video. Investigators can use the command *netstat* to see active connections with remote computer systems when downloading software files. Once the computer system has been seized by investigators, the continuity of the software piracy offense can be determined using the information stored in the registers and files created by the KaZaA application. There is also the KaZAlyser investigation tool, which is used to display IP addresses and other details about file-sharing.

The KaZaA file-sharing program has an important feature for investigators, namely sharing software files as far as possible between computer systems in the same region.

In the case of the offense referred to in Article 195 of Law no 8/1996, the illicit activity consists in unauthorized reproduction of computer programs in any of the following ways: installation, storage, running or execution, display or transmission on the internal network.

In the case of the offense referred to in Article 198 of Law no 8/1996, illicit activity consists in the *production, import, distribution, possession, installation, maintenance or replacement, in any way, of access control devices, either original or pirate, used for program services with conditional access or connection, without right, or connection, without right, of another person to program services with conditional access, or the sale or rent of access control pirate devices.*

In the case of the offense referred to in Article 199 of Law no 8/1996, illicit activity consists in producing, importing, distributing or renting, offering in any way, for sale or for rent, or possessing, without the right to trade them, devices or components which allow the neutralization of technical protection measures or providing services which lead to the neutralization of technical protection measures or neutralizing these technical protection measures, including in the digital environment.

Identifying the work that is the object of software piracy or online piracy illegal actions

The work that is the object of illicit actions of piracy is software that does not have license. According to the provisions of Article 73 of the Law no 8/1996, "the protection of computer programs includes any expression of a program, application programs and operating systems, expressed in any language, either in source-code or object-code, preparatory design material, and textbooks". According to the provisions of art. 74 of Law no 8/1996, "the copyright owner of a computer program shall in particular enjoy the exclusive right to achieve and authorize: the permanent or temporary reproduction of a program, in whole or in part, by any means and in any form, including in the case where reproduction is determined by the installation, storage, running or execution, displaying or transmission on the network; translation, adaptation, arrangement and any other changes to a computer program, as well as the reproduction of the result of such operations, without prejudice to the rights of the person transforming the computer program; distributing and renting the original or the copies in any form of a computer program".

Identifying the author and the circumstances that favored software piracy or online piracy

The active subject of software protection offenses may be any natural person criminally liable. Criminal participation is possible in all forms provided by law (co-author, instigation, complicity). Investigators will determine how offenders have access to confidential information on a computer data storage medium or on a website, starting from the possibility of unauthorized use of software (Stancu 2007, 711).

Identifying the injured person by committing the illicit activity provided by Law no 8/1996

Identification of the person who is the copyright owner of a software and who has been injured by committing one of the offenses provided by Law no 8/1996 is carried out by consulting some records administered by some organizations or bodies with attributions in the field of software protection.

At the level of Romania, this body is the Romanian Copyright Office, which acts as a specialized body under the authority of the Romanian Government, being the sole regulatory authority, recording through national registers, supervision, authorization, arbitration and technical-scientific finding in the field of copyright and related rights, including in the field of software

protection. Please note that the Romanian Copyright Office manages the National Computer Software Registry, in the sense that this registry contains all the software licenses accompanying computer software programs issued by the copyright holders regarding the rights to use these programs. A software license consists of the written authorization that accompanies the computer program, and which is issued by the copyright owner in relation to the right to use that software (Cojanu, 2017, 159).

Identifying practices in the field of software piracy and online piracy investigations

Investigation of offenses related to software protection is carried out according to the forensic investigation methodology of cybercrime. The methodology of software piracy and online piracy forensic investigation is best suited to the peculiarities of cybercrime investigations and includes the following investigation phases (Moise 2011, 213-251): preparation of the investigation; collecting evidence; examination of evidence; evidence analysis; reporting the results.

Identification of digital and physical evidence

Digital evidence represents the "information of probative value that is stored, processed or transmitted in a digital format" (Scientific Working Group on Digital Evidence, 2002, 2).
In the case of software piracy and online piracy, digital evidence consists precisely in the software programs that are used and marketed by offenders without the software license issued by the copyright owner in relation to the right to use that software.

Digital evidence related to software piracy are found on various data carriers (physical evidence), such as: computer systems (desktop computers, laptops, mobile phones), compact discs, DVDs, memory cards, flash drives, optical disks, magnetic disks, computerized agendas, digital cameras.

Regarding digital evidence related to online piracy, we point out that investigators obtain this digital evidence only as a result of the forensic investigation of computer networks, which involves examining digital data in networks within a real time frame. Since computer programs can be uploaded to different web pages or other computer networks, investigators should know that although webpages are written in HTML language, they can be written in languages using scripts (Marcella and Menendez 2008, 155-156). These scripts allow webpages to display content individually for each user. Content can be adapted depending on each user's IP address. Investigators, when investigating a web site for online piracy, they need to establish (Moise 2011, 272-273): identifying the HTML source on a web page; identifying computer data on the web page; locating, searching and seizing the web server. The web server may contain the HTML source as well as the records showing the users' IP addresses, who connect and copy data from the website.

The server can also memorize users' names, passwords, payment methods, and other useful information for investigators when investigating online piracy (Chaikin 2006, 244).

One of the particularities of digital evidence is that it is apparently not obvious, being contained in the IT equipment that stores it. Investigation equipment and specific software are needed to make this evidence available, tangible and usable (Chaikin 2006, 239-256). Another aspect is that this evidence is very fragile, in the sense that it can be changed or can easily disappear by methods that are often at hand of the perpetrators. For this reason, investigators need to take special protective measures to collect, preserve and examine this evidence (Wang 2005, 324).

Identifying the members of the team participating in the investigation of software piracy and online piracy

The team of investigators is generally responsible for the coordination of all activities related to the investigation of software piracy and online piracy. Both due to the special characteristics of the equipment under investigation and the methods used in the forensic investigation process, the members of the investigation team must have the knowledge and skills appropriate to investigate software piracy or online piracy. The team of investigators consists of the following persons: the

prosecutor, who is the head of the investigation team, experts of the Romanian Copyright Office, officers within the competent judicial staff, forensic experts and technical experts.

Identifying the tools needed to investigate software piracy and online piracy

Forensic investigation of software piracy and online piracy requires the use of specific tools. The team of investigators must have enough, high-quality data storage media to enable it to be copied from the analyzed computer system or from another data storage medium. The tools needed to investigate software piracy and online piracy are as follows: hardware tools and software tools.

Ordering and performing evidentiary procedures for investigating software piracy and online piracy

In the case of software piracy and online piracy investigations, forensic expertise, technical-scientific findings and computer searches (Pantea 2016, 278-280) are the most commonly used and conducted evidentiary procedures. The forensic expertise and the technical-scientific finding in the case of pirated computer programs shall be ordered in accordance with the provisions of Article 172 of the Criminal Procedure Code in Romania, in the event that, in order to establish, clarify or assess facts or circumstances relevant to the truth, also required the opinion of an expert. The forensic expertise and the technical-scientific finding in the case of software piracy shall be ordered upon request or ex officio by the criminal prosecution body, by reasoned order, and shall be ordered by the court during trial by reasoned termination. Determining the pirated nature of the software is done in accordance with the provisions of Article 181 paragraph 1 letter k) of Law no 8/1996, which provides that specialists from the Romanian Copyright Office perform expertise for a fee, at the expense of the interested parties or upon the request of the judicial authorities.

We mention that forensic expertise, technical and scientific findings and computer searches in the field of software piracy can be carried out by both the judicial police officers specialized in the field of investigation of cybercrime within the General Inspectorate of Romanian Police - Directorate for Combating Organized Crime, Cybercrime Service, as well as experts from other public institutions, such as National Institute of Forensic Expertise within the Ministry of Justice or the National Forensic Institute within the General Inspectorate of the Romanian Police. After the judicial bodies have indicated the facts and circumstances subject to the assessment and the objectives to be clarified by the experts, the forensic expert's technical-scientific findings and forensic expert reports must provide the judicial authorities with the following important information to prove the existence of software piracy: identifying those programs that do not have software licenses and which are contained by various data storage media; determining the original or pirated nature of that copyrighted software; type and number of pirated software; labeling the data storage media with the manufacturer's code; identifying programs that allow to reproduce and make available to other persons software through peer-to-peer networks; identifying programs that offer the possibility of neutralizing access control measures; the indication of the copyright owners regarding the software they have investigated. (Cojanu 2017, 172).

Carrying out the computer search in the case of software piracy consists of the process of research, discovery, identification and collection of evidence stored in a computer system or storage medium for computer data, made by appropriate technical means and procedures, capable of ensuring the integrity of the information contained therein. Computer searches will be performed on a computer system or data storage medium (CD, DVD, data stick) containing the pirated software. The search warrant is issued by the judge following the computer search provided by the court and includes: the computer system or the data storage support to be searched for the pirated program; the name of the person who illegally uses this pirated software; the period for which the search warrant was issued; the judge's signature and court stamp; date, time and place of issue; the name of the court.

Conclusions

In the field of investigating software piracy and online piracy, investigators must comply with a number of principles of digital evidence (International Organization on Computer Evidence 1999,1): in the process of obtaining digital evidence, the carried out actions should not be modified; when it is necessary for a person to have access to the original digital evidence, this person must be competent from the forensic point of view; all activities in connection with the investigation, storage, examination, or transfer of digital evidence must be entirely recorded in writing, and shall be kept available for evaluation; a person is responsible for all activities in connection with digital evidence as long as they are in possession of it; any organization responsible for investigating, accessing, storing or transferring digital evidence is responsible for compliance with these principles.

Investigating software piracy and online piracy involves two sides: the hardware side and the software side.

The hardware side refers to the investigation of computer systems and data storage media. The software side refers to the investigation of pirated programs and possible other evidence in the data carriers.

References

Cojanu, Toma Cosmin. 2017. *Investigating offences in the field of copyright and related rights.* Craiova: Sitech Publishing House.

Chaikin, David. 2006. "Network investigations of cyber attacks: the limits of digital evidence." *Crime, Law and Social Change,* volume 46, Isseu 4-5, December 2006, Springer Netherlands, Accessed July 1, 2019. https://link.springer.com/article/10.1007%2Fs10611-007-9058-4.

International Organization on Computer Evidence. 1999. Digital Evidence: Standards and Principles. Accessed July 1, 2019. http://www.fbi.gov.

Marcella, Albert J., and Menendez, Doug. 2008. *A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes*. Boca Raton, Florida: Taylor & Francis Group. Auerbach Publications.

Moise, Adrian Cristian. 2011. *The Forensic Investigation Methodology of Cybercrimes*. Bucharest: Universul Juridic Publishing House.

Pantea, Marius. 2016. *Forensics Methodology. Investigating Economic Crime*. Volume I. Bucharest: Pro Universitaria Publishing House.

Savin, Andrej. 2013. *EU Internet Law.* Cheltenham, Glos: Edward Elgar Publishing Limited.

Scientific Working Group on Digital Evidence. 2002. ASCLD Glossary Definitions. Accessed July 1, 2019. http://www.swgde.org.

Stancu, Emilian. 2007. *Criminalistics Treaty*. Fourth Edition. Bucharest: Universul Juridic Publishing House.

Vasiu, Ioana, and Vasiu, Lucian. 2011. *Crime in cyberspace*. Bucharest: Universul Juridic Publishing House.

Wang, Jau-Hwang. 2005. "Cyber Forensics: Issues and Approaches." *Managing Cyber Threats-Issues, Approaches, and Challenges*. New York: Springer Science+Bussiness Media, Inc.