RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
NOVEMBER 2019

DOI:10.5281/zenodo.3550157

The Tactic of Executing Searches

Marilena Cristina Chera

Master in Criminal Sciences at "Dimitrie Cantemir"Christian University of Bucharest, Romania,
marilenachera@yahoo.com

ABSTRACT: The information technology search became one of the investigation ways often met in practice and that is due to the numerous crime, such as corporate crimes or corruption crimes that can be executed through the information technology systems. The ways of crimes found in the information technology crime are carried out by attacks over the information networks and systems. It must be noted that the information technology crimes are not grouped together under one title/chapter, but those are found either in the crimes against property, forgery crimes, and also in the area of crimes against public safety. The ways of executing such are found in most of the information technology crimes. Most of the cases of information technology crimes, the search on the information system, used for executing the crime, might bring out the most important pieces of evidence with the purpose of proving the causal link between the material element and the immediate result of the crime.

KEYWORDS: crime, defendant, evidence, information technology, search

Introduction

The information technology revolution has led to fundamental changes in society and it is very likely that these profound changes will continue to occur (Buzatu 2013, 185).

The search is the probationary procedure by which, in order to pick up, objects, documents or any other objects that can be used as evidence in the criminal process are sought. The search may be domicile, corporal, computer or vehicle; regardless of its nature, the search must be conducted with due respect for dignity, so that it does not constitute a disproportionate interference with private life (Udroiu 2018, 413).

Not ignoring the legal depositions, the particular purpose of the search results also from the fact that, considering the major interest of the justice, the criminal investigation bodies have the possibility to carry out this act even in the conditions where it would mean a violation of the inviolability of the domicile, of the person or the secret of correspondence, as is the case with flagrant offenses.

According to art. 157 para. (1) The Code of Criminal Procedure, the home search or of the goods in the home may be ordered in the following two cases:

a) If there is a reasonable suspicion regarding the commission of an offense, (for which the criminal prosecution was initiated) by an identified, identifiable or unidentified person and it is assumed that conducting the search may lead to the discovery and collection of evidence regarding this offense, the preservation of the traces of the crime or the arrest of the suspect or the accused.

b) If there is a reasonable suspicion regarding the possession of objects or documents related to an offense for which the criminal prosecution was started and it is assumed that conducting the search, it may lead to the discovery and collection of evidence regarding this crime in the preservation of the traces the commission of the crime or the arrest of the suspect or defendant.

The search can only be ordered by the judge of rights and freedoms, by reasoned conclusion, during the criminal prosecution, at the request of the prosecutor or during the trial, by the court, ex officio or at the request of the prosecutor (Udroiu 2018, 334).

The material competence to order the search during the criminal prosecution, belongs to the judge of rights and freedoms from the court whose competence would be to judge the case in the first instance or from the corresponding court in whose grade the district office of the prosecutor's office is located which is part of the prosecutor who carries out or supervises the criminal prosecution.

The functional competence rests with the judge of rights and freedoms, the personal competence rests with the judge of rights and freedoms from the court whose competence is to

judge the case in the first instance by reference to the factual situation retained in the criminal prosecution documents.

The alternative territorial jurisdiction rests with the judge of rights and freedoms from the court whose competence would be to judge the case in the first instance or from the corresponding court in its grade, in which the headquarters of the prosecutor's office of which the prosecutor who supervises or carries out is located prosecution.

The search has been defined in the doctrine as the process by which in certain places the objects and the documents that can be used as evidence in the criminal process are searched, and in case of discovery, they arise from the natural or legal person to which they are found (Udroiu 2018, 413). Unlike the previous regulation, which provided only two categories of searches (home and corporal), two new categories (computer and a vehicle) were introduced in the current regulation.

Computer search involves "research, discovery, identification and collection of evidence stored in a computer system or storage medium of computer data, carried out through appropriate technical means and procedures, so as to ensure the integrity of the information contained therein" (Volonciu 2014, 363). It is necessary to specify that the authorization procedure is similar to the one used in the home search, with the mention that the elements included in the application and in the authorization are less, the object of the activity being a computer system.

If a computer is the result of crime (in North American terminology), an instrument of crime or evidence, the search warrant must target the computer itself and in the alternative the information it holds. The mandate should be as detailed as possible regarding the description of the components to be raised. Where possible, data on the manufacturer, model, other information that may be used for identification shall be included (Vasiu 2001, 38).

Access to a computer system involves entering into a computer system or part of it, or into a storage medium for computer data, for the purpose of obtaining evidence, either at the place where the system or support is accessed, or from a distance, using special software (Udroiu 2018, 416).

Ways of committing cybercrime

To begin with, it is necessary to mention that the operation of computer systems and networks is made up of a series of events, events that involve changing the state of a system or device.

Compared to the idea of computer security "the changes of state" appear the effect of the action directed on some targets (Moise and Stancu 2017, 238). Thus, by way of example, it may be remembered that a computer system was accessed, the action being represented by the user's access control program authentication, according to an identity controlled by username and password.

Thus, for a good understanding, authors of the specialized literature (Moise and Stancu 2017, 238) defined the event as "an action carried out on a target system by which it is intended to change the state of the system".

The forms of perpetration that are encountered in cybercrime are achieved through attacks on computer systems and networks.

The attack on a computer system goes through the following steps:

- Researching the computer system in order to obtain information represents a first step in the computer attack. Thus, this first step aims to obtain important information that can be used in attack such as finding out the type of hardware used, the software version.
- Penetration into the information system. Subsequently, the identification of the target information system and the gathering of information about the respective system starts the launch of the attack in order to enter the system.
- Changing the computer system settings represents the next step after entering the computer system. Through this step the attacker re-enters the already compromised computer system.

- Communication with other information systems. As soon as the system / network has been compromised, the attacker will use them to attack other computer networks / systems.
- Affecting networks and devices involves deleting or modifying files, stealing important data, destroying computer systems or DOS (Denial of service attacks) attacks.

Attacks on computer systems can be carried out by malicious programs (malware) through which is understood the software that enters a computer system without the owner's knowledge and consent (Vasiu 2001, 160). At the doctrine level, the malicious programs have been classified according to their objective (Moise and Stancu 2017, 239): Viruses and worms (Moise and Stancu 2017, 239) are two types of malicious programs, programs whose main objective is to infect the computer system.

Virus means the program that "infects" executable files or object files (Moise and Stancu 2017, 240). As soon as a virus has infected a computer system, it will perform two tasks. The first is to multiply himself by spreading to other computer systems. As soon as it has multiplied by spreading on other computer systems, it will proceed to perform the second task by activating its malicious function.

Worm means a program that seeks to gain the advantage over a vulnerability in an application or operating system in order to penetrate a computer system. As soon as the worm has exploited the vulnerability of a computer system, it will investigate other computer systems that have the same vulnerability.

Compared to the virus, the worm is a standalone program that exists independently of other programs, without needing other programs to run (Amza 2003, 115).

Through the forensic investigation of a computer system, the aim is to ensure a high degree of accuracy of the conclusions that can result from the action. According to the *Introductory Guide for the application of the legal provisions regarding cybercrime, the main features of the investigation activity* are (Moise and Stancu 2017, 246):

- authenticity (proof of the source of provenance);
- credibility (lack of any doubts about the credibility and soundness of the evidence);
- completeness (taking all the existing samples and their integrity);
- lack of interference and contamination of samples as a result of investigation or manipulation of samples after their collection;
- the existence of predefined procedures for situations encountered in practice;
- anticipating the possible criticisms of the methods used, based on the authenticity, credibility, completeness and affectation of the offered evidence;
- the possibility to repeat the tests performed, with identical results being obtained;
- anticipation of problems related to the admissibility of evidence;
- accepting the fact that the research methods used at one point may be subject to changes in the future.

The forensic investigation activity of the information systems involves the use of both the law elements, as well as the information and communications technology in order to collect and analyze the data from the information systems, networks, wireless communications and devices for storing the computer data, so that all these can be used as evidence in a court (Moise and Stancu 2017, 246).

In the case of the emergence of new forms of crime (For example, deception through the computer, cloning of electronic means, for example, computer attacks for collecting data with economic value), to overcome the difficulties of the investigation due to the absence of traces in the classical sense, because the crime between the perpetrator and the injured person does not take place in the real space, but in the virtual one, the reaction of the criminal is to develop new methods and techniques of investigation, to capitalize on the computer traces and to manage the digital samples (Grofu 2019, 116).

Searching in a computer system or a computer data storage medium, also called a computer search, represents the process of researching, discovering, identifying and collecting the samples stored in a computer system or computer data storage medium, carried out by some means. Appropriate techniques and procedures, such as to ensure the integrity of the information contained therein" (Grofu 2019, 117).

Thus, in order to gather evidence, the competent body established by the criminal procedural law, will be able to arrange, whenever necessary, the computer search.

In order to obtain information, with probative value, which are stored, processed or transmitted through a computer system, it is compulsory to have, by the competent judicial bodies, the carrying out of both the home search and the computer search, and, not lastly, the issuing of the criminal investigation bodies of the corresponding mandates.

In this context it should be mentioned that the procedural law of search conflicts with the fundamental rights and freedoms with is individual freedom, the inviolability of the domicile, the inviolability of the secret of correspondence, the right of private property (see art. 23, art. 27, art. 28 and art. 44 of the Romanian Constitution). In this conflict that can be born between the right of the search process and the individual right on the person, home, etc. the procedural law takes precedence, this being the exception. In order to carry out the computer search, the following preparatory activities will be taken into account:

- maintaining a permanent connection with the police units with attributions in the field of cybercrime in order to establish the details regarding the date and place of conduct;
- carrying out the procedure of summoning the person whose information is to be searched, mentioning the date, time and place of the activity as well as announcing the defendants of the suspect or the defendant about it;
- making available the information systems and storage media to be subject to search, and in the end, taking over the sealed and sealed information systems;
- making available all the documents useful for carrying out the computer search, such as: the address from the unit requesting the search, the delegation order from the prosecutor's office, the computer search warrant;
- mention of the purpose of the search for the specialist to perform the search.

The search of an information system can be ordered both in the criminal prosecution phase and in the non-trial phase.

In the phase of criminal prosecution, at the request of the prosecutor, the judge of rights and freedoms from the competent court to judge the case in the first instance or from the corresponding court in its grade, in whose constituency is the headquarters of the prosecutor's office of which the prosecutor is a member or supervise the criminal prosecution will be able, by *reasoned conclusion* to carry out a computer search (Moise and Stancu 2017, 250).

The request of the prosecutor regarding the approval of the search is solved (unlike the procedure for obtaining a home search, art. 158 para. (5) NCPP, which provides for a period of 24 hours - in the case of information technology, there is no regulation within which the request must be resolved) in the council chamber, without summoning the parties, but the prosecutor's participation is mandatory.

The conclusion by which the judge of rights and freedoms rules on the application is not subject to appeal.

The reasoned conclusion of the court will have to contain the standard elements, and the search warrant should contain the same elements, such as "court name, date, time and place of issuance, name, first name and quality of the person who issued the warrant, the period for which it was issued and within which the ordered activity must be performed, the purpose for which it was issued, the computer system or the storage medium of the computer data to be searched, as well as the name of the suspect or the defendant, if known, the signature of the judge and the stamp of the court" (Volonciu 2014, 360).

We should mention that, before starting the criminal investigation, the computer search cannot be arranged. During the trial, the computer search is arranged "by the court by reasoned conclusion, ex officio or at the request of the prosecutor, of the injured party or person, when for the discovery and collection of evidence it is necessary to investigate an information system or a storage medium of the computer data" (Moise and Stancu 2017, 252).

In this case, the warrant for carrying out the computer search will be communicated to the case prosecutor, who has the obligation to execute it. In most cases, this form of search is ordered after the computer system is picked up and transported to a forensic laboratory, as a result of a home search. In case the computer system can be lifted and transported the search was carried out in a forensic laboratory. However, if the computer system or the data storage medium cannot be picked up and transported, the search will be carried out at the place where the computer data storage system or media is located.

When, on the occasion of performing the computer search, it is found "that the sought computer data are contained in another computer system or storage medium of the computer data and are accessible from the initial system or support", the prosecutor has the obligation to order the preservation immediately, copying the identified computer data and will urgently request the completion of the search warrant.

In order to ensure the integrity of the computer data stored on the raised objects, the prosecutor may order the copies to be made, using technical means and appropriate procedures, so as to ensure the integrity of the information contained therein.

This form of search can only be carried out by a specialist, from the judicial bodies or from outside them, only in the presence of the prosecutor or the criminal investigation body.

As a result of performing the computer search, information can be obtained regarding: addresses, audio-video recordings, databases, email correspondence, web pages visited, deleted files, images, etc.

The result of the computer search activity, the possible objections, as well as the answer to these are recorded by the preparation of a report, to which will be attached the statements of the audited persons, other annexes (the photographs taken, the documents taken, screenshots) as well as the Program report. Forensic investigation of the cybercrime that was used in the investigation process.

In the case of cybercrimes, the on-site investigation can be carried out when it is necessary to ascertain the location of the crime, the discovery and fixing of the traces of the crime: establishing the position and status of the material means of evidence and the circumstances in which the cybercrime was committed (Stancu 2010, 351).

In the case of computer crimes, the on-site investigation includes *a static phase investigation and a dynamic phase investigation.*

In the static phase, the research aims to ascertain the state of affairs, not intervening in any form on the apparatus, which should not be started, but not stopped if it works. In the situation where, it is required that the objects be moved, this will be done only after fixing its position by appropriate notations in the minutes, by shooting, filming or sketching, if appropriate.

In the *dynamic phase* the stages of collecting, examining and analyzing the samples can be included, which the investigator must go through in the investigation process (Moise and Stancu 2017, 255). From a technical point of view, in the case of computer crimes, the computer search and the on-site investigation include the same stages / phases of investigation.

The phases of the process of investigation of cybercrimes are as follows (Moise 2011, 213-251): preparation of the investigation; collection of evidence; examining evidence; sample analysis; reporting the results obtained.

In the case of computer crimes, the notification of the criminal prosecution body is the usual one, respectively the notification by complaint or denunciation, as an external notification mode. However, there are also cases of ex officio notification of the criminal prosecution bodies, these being equivalent to a referral, when one becomes aware of the act of a deed by another way than by complaint or denunciation (Buzatu 2013, 194).

Conclusions

The main reason for choosing the theme lies in the fact that, in the last decades, computer searches have become one of the forms of investigation commonly encountered in practice and this is because many crimes, such as business crimes, corruption offenses, can be committed with the help of IT systems.

It should be noted that cybercrimes are not grouped into a single title/chapter, but they are found both in the category of crimes against the patrimony, the crimes of forgery, but also in the field of crimes against the public security. The computer search is an act of criminal prosecution that raises the objects that can constitute evidence regarding the commission of certain forms of crime. At the same time, computer search is the probationary procedure used to obtain digital evidence. With the title, for example, the threat of crime, it can be proven, in certain situations, with the help of emails containing, in the header section, information regarding the IP address of the computer system.

Digital evidence is nothing but that information that is stored, processed or transmitted using the computer system, being accepted by the courts.

In most cases of computer crime, the search of the computer system, used to commit the crime, can provide the most important evidence in order to prove the causal relationship between the material element and the immediate follow-up of the crime.

References

Amza, T. and Amza, C.P. 2003. *Computer Crime*. Bucharest: Lumina Lex Publishing House.

Buzatu, N.-E. 2013. *Forensics*. Bucharest: Pro Universitaria Publishing House.

Grofu, N. 2019. *Criminal Law*. *Tactics.* Bucharest: Didactic and Pedagogical Publishing House.

Moise, A.C. and Stancu, E. 2017. *Forensics. Methodological Elements of Crime Investigation*. Bucharest: Universul Juridic Publishing House, Bucharest.

Moise, A.C. 2011. *Methodology of forensic investigation of cybercrimes.* Bucharest: Universul Juridic Publishing House.

Stancu, E. 2010. *Criminal Law Treaty*, ed. 5th. Bucharest: Universul Juridic Publishing House.

The Code of Romanian Criminal Procedure.

The Constitution of Romania, published in the Official Gazette of Romania, Part. I, no. 767, of October 31, 2003.

Udroiu, M. 2018. *Criminal Procedure, General Part*. Bucharest: C.H. Beck Publishing House.

Vasiu, I. 2001. *Computer Crime*. Bucharest: Nemira Publishing House.

Volonciu, N. et al. 2014. *The New Code of Criminal Procedure. Commented*. Bucharest: Hamangiu Publishing House.