RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
June 6-7, 2024

10.5281/zenodo.12684733

Special Measures to Investigate Computer Crime

Maria Gabriela Zoană

Lecturer PhD, The National University of Science and Technology Politehnica Bucharest, Pitești University Centre, Faculty of Economic Sciences and Law, Romania, av_zoana@yahoo.com

ABSTRACT: Investigating fraud committed through computer systems requires an increasingly elaborate and innovative methodology due to the fact that judicial bodies are forced to keep up with the accelerated development of criminal networks and advanced techniques for committing computer crimes, the Internet becoming a difficult space controllable and immense for victims and offenders due to its cross-border nature. The complexity of forensic investigations is due to the difficulty in identifying the real author of the crime in question and the timely detection of the commission of computer crimes. The vulnerability associated with computer systems and the multiple possibilities of long-distance action by criminals create advanced levers for forensic investigation of this type of crime. The European Union shows a constant concern for limiting and combating computer crime and has created the general legal framework that allows member states to homogenize national legislation by referring to the Council of Europe Convention of 23.11.2001 on computer crime, strengthened by Directive 2013/40/EU of the Parliament European and Council of 12.08.2013 on attacks against computer systems. Recently, the European Parliament adopted on 13.03.2024 the Regulation on Artificial Intelligence, the first harmonized European legislative proposal in the field of artificial intelligence, a regulation that focuses on the major risks that the authorities must consider. New technologies and the scale of the development and use of artificial intelligence create even greater difficulties for judicial bodies in preventing, detecting, investigating and combating computer crimes.

KEYWORDS**:** computer crimes, computer attacks, computer fraud investigation, artificial intelligence, forensic investigation

Vulnerabilities of computer systems and obstacles in the investigation of computer crimes

Vulnerabilities associated with IT systems are most often found in data storage systems, being the most sensitive hardware components and in the event of their failure, the damage is the most significant through the partial or total loss of information. Internet communications are also insecure. Anyone can connect to the communication line and intercept, alter or even divert the data traffic, if there are no methods to encrypt the data, so that if it is intercepted, it cannot be decrypted. In the sense of Directive (EU) 2013/40/EU of the European Parliament and of the Council, by computer system we mean a device or a group of interconnected or approved devices, one or more of which ensures, through a program, the automatic processing of data IT, as well as the IT data stored, processed, recovered or transmitted by this device or group of devices in order to exploit, use, protect and maintain them (Article 2 letter (a) of Directive (EU) 2013/40/EU of the European Parliament and of the Council of 12.08.2013 on attacks against computer systems and replacement of Framework Decision 2005/222/JHA of the Council published in the Official Journal of of the European Union L218 of 14.08.2013). The definition of the computer system has been improved compared to that provided for in the Convention of the Council of Europe of 23.11.2001 on computer crime (Article 1 letter a) of the Council of Europe Convention of 23.11.2001 on computer crime, (published in the Official Gazette of Romania no. 343 of April 20, 2004), according to which computer system means any isolated device or set of interconnected or connected devices, which ensures or one or more many elements ensure, by executing a program, the automatic processing of data.

Computer systems are primarily vulnerable to classic attacks, when an attacker manages to penetrate the premises of the computer systems and steal confidential information (Ghervase 2021, 56). Another vulnerability of IT systems is represented by “natural disasters; earthquakes, floods, fires or accidents such as voltage drops or overvoltages that can lead to the physical destruction of computing equipment” (Leu 2021, 64).

Establishing all the circumstances of the commission of the crime is one of the main objectives of the cybercrime investigation and these circumstances could be: hacking, cracking or phishing. By hacking, we mean penetrating, infiltrating a computer system or breaking into a computer system, with the help of a variety of techniques and programs. By cracking is meant the use of a program and specific techniques to penetrate the passwords of a computer or a computer system. Phishing means stealing someone's identity by means of identification information that is then used in fraud activity.

It is relevant to mention that the obstacles in the investigation of the crime are created not only by those directly or indirectly involved in the commission of the crimes, but even by people who apparently have no direct interest, even are unknown to the criminal, for example hackers, who are prone to carry out on their own initiative, as a sign of solidarity, certain movements on the Internet, in order to endanger the prosecution of other guild colleagues, even unknown ones.

The tools used to create obstacles before the criminal investigation body, characteristic of computer crimes, are also very important. Among these, by way of example, we mention the most frequently encountered ones: software products used to commit the crime, which leave no traces, are instantly deleted and/or encrypt the information; the software that makes the identification of the person inadmissible or the use of intermediate servers, when it is impossible to destroy the traces; programs that cannot always be identified by security systems; remailers, i.e., servers that receive messages with embedded instructions and forward them to the destination email address, deleting all data about the sender; computer data stored remotely; distraction maneuvers (such as cyber-attacks); other technical possibilities of concealing the crime, ensured by various methods and means (for example, blackmail or the certainty that the victim's reputation is affected and then he hides and does not denounce the crime).

Criminal investigation bodies must take specific measures to overcome obstacles in the investigation of computer crimes. Ensuring confidentiality when collecting information on crimes committed and on suspected criminals, but also on procedural actions planned or already carried out by criminal investigation bodies or by other bodies or institutions with which they collaborate is the basic measure taken by the criminal investigation body. This confidentiality can be ensured by limiting or prohibiting the connection/disconnection to the Internet of the IT systems that constitute the object of the crime; by continuing the victim's online activity in order not to draw attention to the investigations carried out; by planning the chronology of the procedural activities, so that the actions against the persons who can disclose the data of the investigations are carried out in the last instance; by carrying out searches or collecting evidence and documents during the period of time when the massive presence of witnesses can be avoided - carrying out the collection of IT systems and devices used in the commission of the crime, even at the initial stage of the criminal process (a measure aimed at preventing the appearance and negative effect of obstacles to the investigation); by submitting to a permanent control of all electronic messages, sent by the subdivision that carries out the investigation on the case; by establishing malfunctions in the information security system of the victim's computer systems, as well as hidden dangers in computer systems accessed without authorization; by collecting data about people who have access to documents and who can take actions to destroy evidence - the criminal investigation body, as well as the judges who have access to the information in the file during the criminal investigation, will have to provide as little information as possible about the investigations carried out and suspect persons in the procedural documents.

Another important measure is the establishment of the general framework and the necessary information for the initiation of the criminal investigation, as well as during the criminal process by planning the implementation of special investigative measures, aimed at obtaining information, which can be used to overcome the impediments regarding the

forensic investigation. Such data can also present elements specific to criminology and can also refer to the personality of the criminal, to the people who can provide help to the perpetrator, to the information regarding the activities planned by the criminal specific to computer crime.

Identifying and verifying the sources from which evidence can be obtained is a basic measure that any criminal investigation body must take into account in order to achieve the principle of finding the truth, even more so in the prosecution of computer crimes, the verification of sources providing evidence is essential, as the samples present a much greater risk of being tampered with.

The professionalism of the investigation team and the good collaboration of the prosecutor of the case with the criminal investigation body, including the forensic investigation team that performs the special work to be investigated, the continuous monitoring of the activity of forensic experts and the verification of the correctness of the information collected by the investigation team, are also vital in the success investigation of a computer crime.

Another specific measure for overcoming obstacles in the investigation of computer crimes could be anticipating the possible obstacles that may appear when collecting materials, as well as the behavior of the criminal, planning and carrying out actions to thwart them, including technical measures: identifying special software, intended to prevent unauthorized access to information, installation of filters.

When there are already obstacles to the progress of the investigation, the prosecuting body should consider planning and carrying out activities to overcome these already existing obstacles, with the involvement of all members of the investigative team, especially IT specialists and when appropriate other specialists with advanced knowledge may be involved with all measures taken to protect the confidentiality of the investigation.

The modern technical possibilities available to criminals allow them to keep cyber-crime under control, to coordinate the actions of accomplices, to direct them, to the extent that they receive urgent signals, and to elaborate, based on the analysis at Cestora, the indications of rigor.

The alibi is also quite a big obstacle in the investigation of computer crimes where we often encounter the so-called digital alibi. The purpose of the false alibi is to thwart the effort of the prosecuting body to establish the truth in the case and to try to influence the evidentiary system in favor of the criminal. By invoking the alibi, the impossibility of participating in the conduct of an illegal activity of the suspect is supported, because he would have been, during the period of time when the investigated illegal activity was carried out, in another place, so that he could not do what he is accused of, for that he physically could not do it. Using the alibi, the suspect proves his innocence by the fact that when the crime was committed, he was somewhere other than the place where the crime was committed, but this is not always true in the case of computer crimes, since they can be committed from any place.

The principle of the existence of traces of any criminal act, a fundamental principle of criminology which consists in the fact that there is no perfect crime, in the sense that any illegal act of man entails changes or material transformations, which in fact represent traces of the crime (traces can be left both the offender and the victim) is also valid in the case of the investigation of computer crimes. No matter how much the computer criminal tries to hide his presence in the online environment, there are always traces. More than that, from the judicial practice, a certain arrogance or pride of the computer criminal has been observed, which has his tendency to be recognized and to claim a higher place in the hierarchy of criminals, in which he brags about his actions carried out in the virtual space, to gain the appreciation of other criminals or those active in the field of activity in which the cybercriminal is interested.

In principle, when they refer to the digital alibi, the criminals reason that, at the time of committing the crime, they were working from their personal computer (or they were using their personal mobile phones, they were in the observation perimeter of the surveillance cameras, they connected to the computer networks through personal authorization), which, in reality, was elsewhere. In such cases, the criminal investigation body must, first of all, carry out the tactical action of hearing the person who invokes the digital alibi (Moise and Stancu 2017, 193). Here, the criminal investigation body is to establish the direct connection between the location of the suspect at the time of the crime and the electronic system located at a distance, in another place, giving rise to the notion of virtual traces.

Forensic scientists can also collect material traces such as fingerprints on the keyboard or traces left by sweat secretions, traces left by human remains, etc. The time of formation of these traces is extremely difficult to establish, due to the permanent interaction of the person with the external devices of the computer system. The ideal traces, however, remain in the mind and consciousness of the person who directly manipulates a concrete computer system.

In the procedure for checking digital alibi versions, the prosecution body identifies whether the suspect has special professional skills in the IT field (the prosecution body's checks start from the offender's studies in the field to the description of his skills and experience, the profile they make by work colleagues, or the employer, the description of the hobbies he has in the field). Following the logical analysis of all the information in a specific case, the criminal investigation body elaborates the versions: the suspect has a digital alibi, the suspect does not have a digital alibi, or the suspect's digital alibi was falsified.

Criminalists can also create a psychological portrait of the suspect along with his identity (name, date, year of birth), as well as phone numbers, e-mail addresses of the person invoking the digital alibi from the information placed by him on the Internet, namely, in social networks (for example, Facebook, Instagram, TikTok and other social networks). Since most of this information is public and easily found on the Internet, there is no need for authorization, which greatly facilitates the work of the criminal investigation body.

The tactics of carrying out specific forensic procedures in the case of computer crimes and the use of IT specialists in forensic procedures specific to the research, discovery and investigation of crimes in the category of computer crime

The prosecutor and in general the lawyer who constitutes the criminal investigation body does not have and cannot have knowledge in all fields, therefore, in order to fulfill his tasks for the success of the investigation and finding out the truth, he usually involves specialists from fields that do not are known to him or in which he has insufficient knowledge. Specialization and current technical progress do not allow the representative of one field to be absolutely competent in another field. From our point of view, the involvement of IT specialists is indispensable in the case of the investigation of computer crimes, and the criminal investigation body will identify the necessary special knowledge in the fields of the specialist that it will attract within the procedural actions, because it is impossible for that specialist to possess complete knowledge in all IT fields.

The criminal investigation body can call on the specialist's knowledge at any time during the criminal investigation, in any judicial procedure, even when preparing the questions that will be addressed to the suspect or at the time of his hearing where the specialist, due to his high knowledge in the field, will not allow him the interviewed person to take the initiative of leading the interrogation and not to distort the meaning of the questions and the nature of the answers, but will manage to keep the hearing within the

limits of the object of the case and to make references to the existing evidence that the specialist discussed before the hearing with the criminal investigation body. It is worth mentioning that there are also disadvantages when the IT specialist is present at the hearing as obstacles could be created in establishing psychological contact between the person being heard and the criminal prosecution body that conducts the hearing, therefore a pre-hearing preparation of the IT specialist by to the research bodies.

The interview tactics must take into account the personality of the interviewee, regardless of whether the suspect, victim or witness is being interviewed. If the victim of the IT crime is a legal person, the employees who had duties related to the investigated act will be heard as witnesses (the network administrator, IT system operator, programmers, persons responsible for IT security, employees responsible for maintenance may be heard IT systems technician, IT department manager, etc.). If the victim is a natural person, the computer systems used by the victim will be identified, the level of IT knowledge of the victim and those related to computer systems in general or the use of complex devices, knowledge of the specifics of the program products installed on the computer, if there is an occasional connection will be checked between the victim and the criminal or an apparently contractual one, how he found out about the crime committed and the source of information, if there was visual contact with the perpetrator of the crime and under what conditions and any other aspects that can lead to the success of the forensic investigation.

We believe that in certain situations it is advisable for the specialist to participate even in the procedure of carrying out the on-site investigation where it can be useful to identify and explain the circumstances related to the case, to fix and collect evidence, as well as to monitor what the suspect reported, so that to avoid the creation of a wrong track by the criminal investigation body.

As I have shown before, an effective means of forensic investigation specific to computer crimes is the search immediately after the start of the criminal investigation, because this fact will ensure the detection and collection of evidence, the means and tools of the crime, a judicial procedure in which the participation of the IT specialist is welcome if the criminal prosecution body considers that it does not have the necessary intellectual capacity to detect all the evidence in the field of computer crime. At the European level, the general framework for the specificity of searches carried out in the case of computer crimes was established, which creates the right for member states to search an computer system and the computer data stored in it, as well as any computer storage medium (See art. 19 of the Council of Europe Convention of 23.11.2001 on computer crime, published in the Official Gazette of Romania no. 343 of April 20, 2004).

During the search or the collection of objects and documents, in addition to the specific rules of criminal procedural law, the forensic tactic presupposes the observance of certain specific rules: once they arrive at the scene, the team members must enter the room quickly and unexpectedly, in order to prevent the destruction of data computers, and the people present must be prohibited from touching and using electronic and communication devices: computers, data storage media, mobile phones, tablets, fax and others. Immediately after the team members enter the room, the security of the computer systems as well as the power source must be ensured to prevent the deletion of information. Body searches can also be carried out if there are suspicions that certain persons may hide communication equipment or objects intended for the destruction of computer data. When there are suspicions that accomplices of the criminal, who are outside the area of the procedural action, have been notified about the search, it is immediately necessary to disconnect network connections from electronic devices (disconnect network cables, disconnect modems and routers, stop using the Wi-Fi mode Be and the transmission of data packets). The results of the research at the front of the horse will also be made concrete by making a sketch or a detailed scheme regarding the assembly, especially of the peripheral cables, in

order to ensure the possibility of reconstructing the operation mode of the entire system. In the case of criminal participation, ideally the search should be carried out simultaneously at each of the participants. A specific measure would be to draw up a table with IT specialists related to the subject of the search, officially and unofficially employed), who are to be heard immediately and separately regarding their duties and the data stored in the IT systems (ideally it would be not be able to communicate with each other even during the search).

The European legislator's concern about information crime. Results and conclusions

Each member state of the European Union has regulated in its own legislation the crimes specific to computer crime in accordance with the recommendations of Directive (EU) 2013/40/EU of the European Parliament and of the Council which establishes the general framework for four types of crimes (See art. 3-6 of Directive (EU) 2013/40/EU of the European Parliament and of the Council of 12.08.2013 on attacks against information systems and replacement of Framework Decision 2005/222/JHA of the Council published in the Official Journal of the European Union L218 from 14.08.2013): illegal access to computer systems, illegal damage to system integrity, full damage to data integrity and illegal interception, ensuring the legal framework for criminal procedural aspects and sanctions. In this context, for example, Romania has legislated in the criminal code (See art. 249 and Chapter VI: Offenses against the security and integrity of IT systems and data, art. 360 – 365 of the Romanian Criminal Code adopted by Law no. 286/2009 published in the Official Gazette of Romania no. 510/2019, subsequently amended by Law no. 187/2012 for the implementation of the criminal code and with successive amendments until 01.07.2024) a series of specific crimes: computer fraud (art. 249), illegal access to a computer system (art. 360), illegal interception of a transmission of computer data (art. 361), altering the integrity of computer data (art. 362), disrupting the functioning of computer systems (art. 363), unauthorized transfer of computer data (art. 364), illegal operations with computer devices or programs (art. 365).

Cybercriminals are people with a high flexibility of operational transition from the real dimension to the virtual one, from a relationship mediated by an emotional-physical space to a relationship mediated by an emotional-artificial space, they are characterized by a diminished altered perception on the illegality of their behavior, the damage caused, the risks of being reported, discovered and sanctioned, with or without technical knowledge in the IT field, with a predominantly non-violent profile, having a common language, with specific terminology, and a criminal motivation diversified (whether material, sexual, ideological, political, status-obsessed or investigative).

Any computer system, no matter how sophisticated the security measures are, is subject to the risk of unauthorized access, as has been proven in practice. For example, on September 18, 1996, the C.I.A. Web page was accessed without authorization - considered a true bastion of technology - which led to its closure, the next morning, by the agency's representatives. Also, in August 1996, the website of the U.S. Ministry of Justice was "hacked". In both cases the authors remained unidentified (Oancea n.d., 2).

At the level of the European Union, the mission of achieving a high level of cyber security throughout Europe falls to the European Union Agency for Cyber Security, ENISA (2024). Among other tasks, the European Union Agency for Cybersecurity cooperates with Member States and EU bodies and helps Europe to prepare for tomorrow's cyber challenges and to ensure the digital security of European society and its citizens in a world that has become hyperconnected and where cybercriminals pose a significant threat to the internal security of the European Union and the online security of its citizens.

The Recovery Plan for Europe (2024) exposes the vulnerabilities to cybercrime and cyberattacks faced by Member States, which shows the European Union's growing concern about this increasingly difficult to control criminal phenomenon.

Also, at the European level, the first harmonized legislative proposal in the field of artificial intelligence was adopted, the Regulation on Artificial Intelligence (European Parliament 2019-2024) regulation focusing on risks major issues that the authorities must take into account in relation to new technologies and taking into account the explosion in the development of artificial intelligence that will certainly create new challenges and great and unexpected difficulties for judicial bodies in the prevention, detection, investigation and combating of computer crimes.

In **conclusion**, the measures to investigate computer crimes have a special specificity due to the way in which the crimes are committed, namely in the online environment, that is why the forensic investigation is supplemented with methods adapted to the specifics of computer crime and the mode of operation of computer criminals. Considering the permanent modernization of computer systems, new ways of committing crimes appear, therefore the co-opting of specialists with high professional training in the IT domain is essential, as criminal prosecution bodies do not have the necessary technical training specific to the computer field. Although the criminal investigation bodies are making sustained efforts, and worldwide there is international judicial cooperation in this regulated field, computer crime is gaining momentum, and the increased use of artificial intelligence on the one hand helps forensics to detect crimes and their authors, on the other hand part creates a new criminal territory for criminals. The most important thing is for the legislator of each state, the European legislator, but also worldwide to create strong and always updated rules and procedures to combat the criminal phenomenon.

References

Directive 2013/40/EU of the European Parliament and of the Council of 12.08.2013 on attacks against information systems and replacing Framework Decision 2005/222/JHA of the Council published in the Official Journal of the European Union L218 of 14.08.2013.

European Commission. 2024. "The Recovery Plan for Europe." https://commission.europa.eu/strategy-and-policy/recovery-plan-europe_ro.

European Parliament. 2019-2024. Artificial Intelligence Act, P9_TA(2024)0138 - Legislative resolution of the European Parliament of 13 March 2024 regarding the proposal for a regulation of the European Parliament and the Council of establishing harmonized rules on Artificial Intelligence (Artificial Intelligence Law) and amending certain Union legislation (COM(2021)0206 – C9-0146/2021 – 2021/0106(COD)). https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138_RO.pdf.

European Union Agency for Cyber Security (ENISA). 2024. "About ENISA." https://www.enisa.europa.eu/about-enisa/about/ro.

European Union. 2023. Convention on cybercrime." https://eur-lex.europa.eu/RO/legal-content/summary/convention-on-cybercrime.html.

Ghervase, Denis Gabriela. 2021. *Information security and the internet – computer crime.* Craiova: Universitaria Publishing House.

Leu, C. 2021. "On-site investigation in the case of computer crimes (Computer crime)". Volume: *Forensic investigation of the crime scene.* Bucharest: Luceafărul Publishing House.

Moise, Adrian Cristian and Stancu Emilian. 2017. *Criminalistics. Methodological elements of criminal investigation,* Bucharest: Universul Juridic Publishing House.

Oancea, Dorinel. n.d. "Computer Crime." Available at http://old.mpublic.ro/jurisprudenta/publicatii/criminalitatea_informatica.pdf, 2

The Convention of the Council of Europe of 23.11.2001 regarding computer crime, published in the Official Gazette of Romania no. 343 of April 20, 2004.

The Romanian Criminal Code adopted by Law no. 286/2009 published in the Official Gazette of Romania no. 510/2019, subsequently amended by Law no. 187/2012 for the implementation of the criminal code and with successive amendments until 01.07.2024.