DE GRUYTER OPEN
JOURNAL OF LEGAL STUDIES
"Vasile Goldiş" Western University of Arad
J. L. S.
DOI: 10.1515/jles-2015-0011

PROCEDURAL ASPECTS OF CYBERCRIME INVESTIGATION

Alin Teodorus Dragan
"Vasile Goldis" Western University of Arad

Abstract: Romanian legislation has had to adapt to new challenges. Following the ratification by our country of the provisions of the Council of Europe on cybercrime, in addition to substantive law provisions, procedural provisions have been introduced, which are intended to regulate the activity of criminal investigation bodies in investigating cybercrime offences.
Keywords: computer systems, computer data, internet

1. Introduction

The creation of computer technology, with an enormous growth and functional potential, its implementation in a variety of social, economic or managerial activities, together with the exponential growth of the value of information, have imposed the necessity of the legal regulation of processes occurring in the sphere of the computerization of human society.

2. Theoretical considerations regarding the procedural aspects of the investigation of cybercrime in the new Criminal Procedure Code (CPC)

The current regulation allows for *the investigation of computer data and systems* in three ways:
- access to a computer (information) system [Art. 138 para. (1) CPC];
- preservation of the computer data (Art. 154 CPC);
- computer search (Art. 168 CPC).

There are differences and similarities between the three forms of investigation, in terms of the scope of the activity, as well as in terms of the authorization procedures and, not least, in material terms, of bringing evidence before the court. The three forms may coexist in the same criminal file, and may be used as steps in a wider process, starting with access to a computer system, followed by the preservation of the data found in the system and their subsequent exploitation through a computer search, or they may be used individually, unrelated to each other, since they are not conditioned by one another[1].

2.1 Access to a computer system is referred to in Art. 138 para. (1), as part of the special means of surveillance or investigation, and is defined in para. (3) of the same article as entering, without notifying the owner or user, into the software running on a computer.

Computer system means any devices or group of devices that are interconnected or have an operational relation, one or more of which ensure the automatic processing of data by means of a computer program. The computer system is open, when it is interconnected with other systems and can be accessed by an indeterminate number of users, or closed, when it operates in a strictly limited field and can be accessed by an indeterminate number of users[2].

According to para. (5) of the same article, *computer data* means any representation of facts, information in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function.

This evidence-gathering procedure has confidentiality as a specific characteristic, as opposed to the search of a computer system, in the sense that the person concerned is not notified and does not participate in the work of the judicial bodies. It takes into account previous computer data, as well as those created during the monitoring.

Penetration can be achieved by using software of the Trojan horse type, which is installed in a computer and communicates all data run on that computer system, but also remotely, by using the Internet connection used by the user, or through the direct installation of key logger software, where there is access to the respective system.

In other words, access to a computer system can be achieved at physical and/or logical level[3]:

- at physical level, access involves interaction with the hardware (the physical part) of the information system (components);
- at logical level, access involves interaction with the software (the logical part) of the information system (software/applications).

The authorization of this activity will be achieved through the issue of a technical surveillance warrant upon the prosecutor's request, by the competent judge of rights and freedoms. The request will be settled on the same day in closed session, without summoning the parties and with the prosecutor's mandatory participation. The handling of the prosecutor's request for technical surveillance arrangements is a non-public procedure, given the confidential nature of this evidence-gathering process.

Technical surveillance can be ordered in the course of criminal prosecution, according to Art. 140 para. (1), CPC, for a maximum period of 30 days. The technical surveillance warrant may be extended, for reasons duly substantiated, by the judge rights and freedoms of the competent court, upon the prosecutor's reasoned request, but each extension may not exceed 30 days. All these extensions, according to Art. 144 para. (3) CPC, may not exceed 6 months with regard to the same person and the same offence.

Activity authorization is a first step in administering the rules of evidence, because, after finding the evidence, it must be collected and brought before the court, this being achieved through the subsequent two steps in the administration of evidence, namely the preservation of the computer data, followed by a computer search.

2.2 The next step, after access to a computer system, is the **preservation of the computer data**. If the criminal prosecution body has information regarding the suspect's criminal activity, which is carried out by means of a computer system or from a computer system, it may order the preservation of the computer data by the communication service provider.
Service provider shall mean[4]:
- any natural or legal person that provides users with the possibility to communicate by means of computer systems;
- any natural or legal person that processes or stores computer data.
The preservation of traffic data may lead to the identification of the person who sent the respective data. Crimes committed by means of computer systems may be committed as a result of the transmission of communications by computer systems. Determining the source or destination of such communications can help identify the perpetrators. In order to determine the source or destination of such communications, traffic data retention is essential. These data are deleted automatically after a certain amount of time by system administrators, so that, unless there is an express order to preserve it, valuable information may be lost[5].
The evidence-gathering procedure of preserving computer data involves keeping the already existing data, obtained through a computer system and stored on a particular medium, so as to avoid their alteration, degradation or deletion.
Thus, the preservation of computer data is an evidence-gathering procedure which ensures the unaltered maintenance of such data by providers of public electronic communications networks or providers of publicly available electronic communications in order to make them available for the judicial bodies[6].
A person's activity on the Internet is recorded from the time of computer startup until its disconnection. All activities carried out on the computer and the Internet remain recorded in the so-called "logs", which are genuine traces that the programs record with regard to their activity. Activities taking place on the personal computer remain stored on it and may be viewed in detail by using software specialized in finding activity history, such as, for instance, USBDeview, which provides information on all devices that have been connected to that system in the course of time.
The activities carried out on the Internet remain stored, recorded on the personal computer, in the memory of the routers, as well as in the memory of the computer systems that manage traffic on behalf of the communication service provider. The

activities carried out on certain websites or database storage systems are stored in personal computers (user), information transfer systems (Internet service provider / ISP), the respective websites and the databases accessed. Each of these systems collects user activity data, whether s/he wants it or not[7].

The preservation of such data regarding a user's activities may be achieved by the prosecutor at the level of the communication service provider or of the website owner or the company hosting the database accessed.

The following conditions must be fulfilled in order to have the measure of computer data retention imposed:

- the criminal prosecution should have been initiated;
- there should be reasonable suspicion about the preparation or commission of a criminal offence;
- the stored computer data should be useful to the case;
- there should be a danger of loss or alteration of the computer data.

According to art. 154 CPC, the preservation is ordered by the prosecutor who performs the surveillance or the criminal investigation, *ex officio*, or at the request of the criminal investigation body, for a maximum period of 60 days, through an ordinance. The preservation measure may be extended, for well-grounded, justified reasons, by the prosecutor, only once, for a maximum period of 30 days.

The ordinance must include, in addition to the general mentions, the following: the providers of public electronic communications networks or providers of publicly available electronic communications services who possess or control the computer data; the name of the offender, suspect or defendant, if known; the description of the data to be preserved; the duration for which it was issued, the mention of the obligation of the person or providers of public electronic communication services or providers of publicly available electronic communications services to immediately preserve the computer data indicated and to maintain their integrity while observing confidentiality.

The prosecutor's ordinance shall be transmitted at once to any provider of public electronic communications networks or provider of publicly available electronic communications that possesses or controls the computer data.

Within a maximum period of 90 days during which these data may be stored, to the extent that the computer data have been preserved, the prosecutor may request the judge for rights and freedoms prior authorization in view of requesting the transmission of such data. The prosecutor also has the possibility to order the ending of computer data preservation.

The judge for rights and freedoms will rule within 48 hours with regard to the request for data transmission submitted by the criminal prosecution bodies, through a reasoned ruling, in closed session.

By the end of the criminal prosecution, the prosecutor has the obligation to notify in writing the person against whom the criminal prosecution is carried out and whose data have been preserved.

2.3 The third step in the prosecutor's activity may be that of the removal of the computer system used to access the Internet or by means of which the criminal offence has been carried out, through the ***computer search procedure*.**
This procedure consists in opening the system and checking its information content, investigation, detection, identification and gathering of evidence stored in a computer system or data storage medium, achieved through appropriate technical means and procedures, so as to ensure the integrity of the information contained therein[8].
The search is a procedural act intended for the finding and seizure of items containing or bearing traces of a crime, material evidence, records, either known or unknown to the judicial body which may serve to finding the truth[9].
Depending on its relation to the development of criminal proceedings, the search may be:
- judicial (house/premises search, body search, search of a vehicle and computer search);
- extrajudicial (customs search, search conducted upon entering a public institution, airport, sports complex, etc.).
As a common rule applying to the judicial search, Art. 156 para. (2) of the Criminal Procedure Code provides that the search should be carried out with dignity, without involving a disproportionate interference with private life.
As for the computer search, this is also considered as an evidence-gathering procedure consisting in the investigation of a computer system or a computer data storage medium, in order to detect and gather the evidence necessary to resolving the case (collecting digital evidence – electronic information with evidentiary value stored or transmitted in digital format – regarding a criminal offence, the preservation through copying of computer data containing traces of the criminal offence, where there is a risk of loss or alteration thereof)[10].
The computer search should be ordered only when there are reasonable grounds to suspect that the computer system or the computer data storage medium regarding which the performance of a search is requested contains evidence of the crime in relation to which the criminal prosecution was initiated and the measure is proportionate to the aim pursued[11].
The phrase "reasonable grounds" may be defined as the existence of data, information which might convince an objective and impartial observer that it is possible for a certain person to have committed a criminal offence.

The second condition involves checking the proportionality of the measure with fundamental rights and freedoms restriction, given the particular circumstances of the case, the importance of the information or evidence to be obtained or the seriousness of the offence[12].

Computer search cannot be ordered before initiating criminal prosecution. For the ordering of the computer search it is not required that the criminal prosecution body should have ordered in advance the continuation of criminal prosecution against the suspect or the initiation of criminal action[13].

Before conducting a computer search, three important aspects should be considered, as follows[14]:

- when requesting the authorization to search, there should be a mention of the fact that the electronic storage media are also going to be checked;
- the place where the analysis of evidence is to be performed must be determined before the beginning of the computer search. This could be a laboratory or even the place where the evidence was discovered;
- the electronic media undergoing the search are as follows: stand-alone computers, computer networks and removable storage media.

There are cases where, as a result of the interconnection that exists between computer systems, the data stored in another computer system than the one subjected to the search may be accessed from the console of the computer system being searched. In this case, the search may be extended, if authorized, to also include the computer system networked with the computer system being searched[15].

The following conditions must be fulfilled in order to impose the carrying out of a computer search:

- criminal prosecution should have been initiated;
- it should be necessary for the discovery and gathering of evidence by searching a computer system or a computer data storage medium.

The power to order the computer search belongs to the judge for rights and freedoms of the court that had jurisdiction to hear the case at first instance or the court of the same level in the jurisdiction of which is located the prosecutor's office to which belongs the prosecutor conducting or supervising the criminal prosecution, according to Art. 168 para. (2) CPC.

The request for the approval of a computer search may be submitted by:

- the prosecutor, during criminal prosecution [Art. 168 para. (2) CPC]
- the prosecutor, the parties or the aggrieved person, during the trial [Art. 168 para. (16) CPC].

It should be stressed out that it is only during the trial that the parties or the aggrieved person may ask the court to order a computer search. During the criminal prosecution, the parties or the aggrieved person may not ask the judge for rights

and freedoms to order a computer search but, if they consider such a search might be useful, they may submit to the prosecutor (who conducts or supervises the criminal prosecution) a request to that effect[16].

The prosecutor submits the request for the approval of a computer search together with the case file to the judge for rights and freedoms. The request shall be handled in closed session, without summoning the parties, the prosecutor's participation being mandatory. The judge for rights and freedoms orders through a ruling the admission of the request, when s/he considers it well-grounded, approves the carrying out of the computer search and issues the search warrant immediately. The legislator did not set a validity time period for the warrant, but did provide that the validity period of the warrant should be specified in the content of the ruling for the approval of the computer search[17].

The court ruling must include:

a) the name of the court;

b) the date, time and place of issuance;

c) the surname, forename and capacity of the person who issued the warrant;

d) the period for which the warrant was issued and during which the activity ordered must be carried out;

e) the purpose for which it was issued;

f) the computer system or computer data storage medium to be searched, as well as the name of the suspect or defendant, if known;

g) the judge's signature and the stamp of the court.

The ruling by which the judge for rights and freedoms rules with regard to the request for the approval of the computer search is not subject to any means of appeal.

It should be specified that the identification of the computer system or the data storage medium is a priority, especially in the case of searching headquarters with multiple computer systems or multiple data carriers/media.

According to Art. 168 para. (12) CPC, the search of a computer system or a computer data storage medium should be performed by a specialist working within the judicial bodies or outside them, in the presence of the prosecutor or of the criminal investigation bodies, as well as the suspect or defendant, who is informed that s/he is entitled to a lawyer's assistance throughout the conduct of the computer search.

If the presence of a lawyer is requested, the beginning of the computer search is postponed until the lawyer's arrival, but for no more than two hours from the time at which this right was communicated. In exceptional cases, requiring the conduct of an emergency computer search, or if the lawyer cannot be contacted, the computer search may begin before the expiry of the two hour-period.

The person whose computer system or computer data storage medium is searched will be allowed to be assisted or represented by a person of trust. When the person whose computer system or computer data storage medium is detained or under arrest, s/he will be brought to the place of the computer search. If the person cannot be brought on site, the computer search should be carried out in the presence of a representative or assisting witness. The presence of an assisting witness is mandatory if nobody is present at the place of conducting the computer search[18].

The preparation of a computer search involves compliance with the following rules[19]:

- collecting information regarding the computer systems to be searched, the type of data storage, the location of the equipment and the storage devices;
- choosing the timing for the carrying out of the computer search, which depends on two factors: the state of the computer system and the presence or absence of certain persons;
- setting up the team participating in the search of the computer system; in addition to investigators, IT specialists must also attend;
- establishing the technical means to be used: software programs, tools, etc.

The computer search report drafted after performing the search should include:

- the name of the person whose computer system or computer data storage media were seized or the name of the person whose computer system is investigated;
- the name of the person who conducted the search;
- the names of the persons present during the search;
- a description and listing of the computer systems or computer data storage media to be subjected to the search;
- a description and listing of the activities carried out;
- a description and listing of the computer data found during the search;
- the signature or stamp of the person who conducted the search;
- the signature of the persons present during the search.

The computer search may be performed in two ways:

- by seizing the computer system;
- without seizing the computer system.

For the first variant of computer search, the judicial bodies must seize the computer system from the suspect or defendant's home or office. In view of carrying out the search ordered, and ensuring the integrity of the data stored on the given objects, the prosecutor orders that copies should be made, which should serve as means of evidence. The copies should be made by using appropriate technical means and procedures, so as to ensure the integrity of the information contained therein[20].

The second variant of computer search regards the situation where files that might contain evidence are hosted on online storage systems, through the rental by the suspect or defendant of an information storage space. In this case, the information

is placed on complex systems, with very high storage capacity, along with other information from other users. The seizure of the computer system and its delivery to the investigative bodies would render the company in question unable to operate anymore, so a variant that may be used instead is to copy the entire content of the suspect or defendant's information, sign the respective files with an electronic signature to prevent their alteration and transmit them in view of their analysis[21].
The results of the computer search benefit from an increased confidentiality status: on the one hand, the judicial bodies must make sure that the facts and circumstances of the suspect or defendant's personal life do not unduly become public. On the other hand, if during the computer search, classified information is discovered, related or not to the offence being investigated, its secrecy must be preserved, but not in relation to the judicial bodies, which have a right of access to classified information[22].

3. Conclusions

Computer systems are not only the target of criminals but also the instrument by which other crimes are committed, or they just facilitate through their functions the committing of traditional crimes. Consequently, many of the investigations of traditional crimes (regardless of their nature) will include computer systems which may contain data about the motivation, identity, location, connections of the perpetrators or accomplices, and may thus facilitate the completion of the respective investigations.

Notes

[1]Nicolae Volonciu (coordinator), Andreea Simona Uzlau, Raluca Morosanu, Victor Vaduva, Daniel Atasiei, Cristinel Ghicheci, Corina Voicu, Georgiana Tudor, Teodor-Viorel Gheorghe, Catalin Mihai Chirita, *Noul cod de procedura penala comentat (The New Criminal Procedure Code Annotated)*, 2nd edition, Ed. Hamangiu (Publishing House), Bucharest, 2015, p. 381
[2]M. Udroiu (coordinator), A. Andone Bontas, G. Bodoroncea, M. Bulancea, V. Constantinescu, D. Gradinaru, C. Jderu, I. Kuglay, C. Mocanu, I. Postelnicu, I. Tocan, Ar. R. Trandafir, *Codul de procedura penala. Comentariu pe articole (Criminal Procedure Code. Comments by Articles)*, Ed. C.. H. Beck (Publishing House), Bucharest, 2015, p. 489
[3]Gheorghe-Iulian Ionita, *Accesul la un sistem informatic si recursul in interesul legii formulat in aceasta materie (Access to a Computer System and Referral in the Interests of the Law Submitted in this Matter)*, in Revista de drept penal (Criminal Law Journal), issue no. 4/2013, p. 113
[4]Mihai-Adrian Hotca (coordinator), Mirela Gorunescu, Norel Neagu, Maxim Dobrinoiu, Radu-Florin Geamanu, *Infractiuni prevazute in legi speciale.*

Comentarii si explicatii (Offences under Special Laws. Comments and Explanations), 3rd edition, Editura C.H. Beck (Publishing House), Bucharest, 2013, p. 379

[5]Mihai Dobrinoiu, *Infractiuni in domeniul informatic (Cybercrime)*, Ed. C.H. Beck (Publishing House), Bucharest, 2006, p. 280

[6]Mihai Olariu, Catalin Marin, *Drept procesual penal. Partea generala (Criminal Procedure Law. The General Part)*, Ed. Universul Juridic (Publishing House), Bucharest, 2015, p. 254

[7]N. Volonciu and collaborators, *op. cit*., p. 382

[8]N. Volonciu and collaborators, *op. cit*., p. 383

[9]Emilian Stancu, *Tratat de criminalistica (Forensic Science Treatise)*, 3rd edition, Ed. Universul Juridic (Publishing House), Bucharest, 2004, p. 449

[10]Laura Codruta Kovesi, *Accesul si supravegherea sistemelor de telecomunicatii sau informatice. Mijloace de proba (Access and Surveillance of Telecommunications or Computer Systems. Means of Evidence)*, in Dreptul (Law), issue no. 7/2003, p. 143

[11]Adrian Cristian. Moise, *Metodologia investigarii criminalistice a infractiunilor informatice (Methodology of Cybercrime Forensic Investigation)*, Ed. Universul Juridic (Publishing House), Bucharest, 2011, p. 205

[12]Rodica, Aida Popa, *Aspecte teoretice si practice referitoare la metodele speciale de supraveghere sau cercetare prevazute in Codul de procedura penala (Theoretical and Practical Aspects related to Special Surveillance or Investigation Methods Set Out in the Criminal Procedure Code)*, in Dreptul (Law), issue no. 6/2015, p. 178

[13]M. Udroiu and collaborators, *op. cit*., p. 489

[14]Simona Lungu, Mihaela Tilea, Dan Voinea, *Cercetarea la fata locului in cazul infractiunilor savarsite prin mijloace electronice (Crime Scene Investigation in the Case of Crimes Committed by Electronic Means)*, article published in the volume „Investigarea criminalistica a locului faptei" ("Crime Scene Forensic Investigation"), Asociatia Criminalistilor din Romania (Romanian Forensic Association), Ed. Luceafarul (Publishing House), Bucharest, 2004, pp. 409-410

[15]A.C. Moise, *op. cit.*, p. 206

[16]Gheorghe-Iulian Ionita, *Aspecte procesual penale si tehnice referitoare la perchezitia informatica (Criminal Procedural and Technical Aspects Related to the Computer Search)*, in Dreptul (Law), issue no. 12/2014, p. 208

[17]Ion Poiana, Ioana Pacurariu, *Drept procesual penal, partea generala (Criminal Procedure Law, the General Part)*, Ed. Universul juridic (Publishing House), Bucharest, 2014, p. 156

[18]Emilian Stancu, Adrian Cristian Moise, *Criminalistica. Elemente de tehnica si de tactica a investigarii penale (Forensic Science. Technical and Tactical Elements of*

a Criminal Investigation), Ed. Universul juridic (Publishing House), Bucharest, 2014, pp. 266-267

[19]Gheorghe Alecu, Alexei Barbaneagra, *Reglementarea penala si investigarea criminalistica a infractiunilor din domeniul informatic (Criminal Law Regulation and Forensic Investigation of Criminal Offences in the Computer Field)*, Ed. Penguin Book (Publishing House), Bucharest, 2006, pp. 224-225

[20]Anca-Lelia Lorincz, *Drept procesual penal (Criminal Procedure Law), Vol. I*, Ed. Universul Juridic (Publishing House), Bucharest, 2015, p. 220

[21]Nicolae Volonciu and collaborators, *op. cit.*, p. 367

[22]According to the Decision of the Superior Council of Magistracy no. 140/2014 approving the Regulation on the access of judges, prosecutors and assistant magistrates of the High Court of Cassation and Justice to classified information, state secrets and intelligence service secrets (www.csm1909.ro)

Bibliography

Treatises, courses, monographs

1. Nicolae Volonciu (coordinator), Andreea Simona Uzlau, Raluca Morosanu, Victor Vaduva, Daniel Atasiei, Cristinel Ghicheci, Corina Voicu, Georgiana Tudor, Teodor-Viorel Gheorghe, Catalin Mihai Chirita, *Noul cod de procedura penala comentat (The New Criminal Procedure Code Annotated)*, 2nd edition, Ed. Hamangiu (Publishing House), Bucharest, 2015

2. M. Udroiu (coordinator), A. Andone Bontas, G. Bodoroncea, M. Bulancea, V. Constantinescu, D. Gradinaru, C. Jderu, I. Kuglay, C. Mocanu, I. Postelnicu, I. Tocan, Ar. R. Trandafir, *Codul de procedura penala. Comentariu pe articole (Criminal Procedure Code. Comments by Articles)*, Ed. C.. H. Beck (Publishing House), Bucharest, 2015

3. Mihai-Adrian Hotca (coordinator), Mirela Gorunescu, Norel Neagu, Maxim Dobrinoiu, Radu-Florin Geamanu, *Infractiuni prevazute in legi speciale. Comentarii si explicatii (Offences under Special Laws. Comments and Explanations)*, 3rd edition, Editura C.H. Beck (Publishing House), Bucharest, 2013

4. Mihai Dobrinoiu, *Infractiuni in domeniul informatic (Cybercrime)*, Ed. C.H. Beck (Publishing House), Bucharest, 2006

5. Mihai Olariu, Catalin Marin, *Drept procesual penal. Partea generala (Criminal Procedure Law. The General Part)*, Ed. Universul Juridic (Publishing House), Bucharest, 2015

6. Emilian Stancu, *Tratat de criminalistica, (Forensic Science Treatise)*, 3rd edition, Ed. Universul Juridic (Publishing House), Bucharest, 2004

7. Adrian Cristian Moise, *Metodologia investigarii criminalistice a infractiunilor informatice (Methodology of Cybercrime Forensic Investigation)*, Ed. Universul Juridic (Publishing House), Bucharest, 2011

8. Ion Poiana, Ioana Pacurariu, *Drept procesual penal, partea generala (Criminal Procedure Law, the General Part)*, Ed. Universul juridic (Publishing House), Bucharest, 2014
9. Emilian Stancu, Adrian Cristian Moise, *Criminalistica. Elemente de tehnica si de tactica a investigarii penale (Forensic Science. Technical and Tactical Elements of a Criminal Investigation)*, Ed. Universul juridic (Publishing House), Bucharest, 2014
10. Gheorghe Alecu, Alexei Barbaneagra, *Reglementarea penala si investigarea criminalistica a infractiunilor din domeniul informatic (Criminal Law Regulation and Forensic Investigation of Criminal Offences in the Computer Field)*, Ed. Penguin Book (Publishing House), Bucharest
11. Anca-Lelia Lorincz, *Drept procesual penal (Criminal Procedure Law), Vol. I*, Ed. Universul Juridic (Publishing House), Bucharest, 2015

Specialized journals
12. Gheorghe-Iulian Ionita, *Accesul la un sistem informatic si recursul in interesul legii formulat in aceasta materie (Access to a Computer System and Referral in the Interests of the Law Submitted in this Matter)*, in Revista de drept penal (Criminal Law Journal), issue no. 4/2013
13. Gheorghe-Iulian Ionita, *Aspecte procesual penale si tehnice referitoare la perchezitia informatica (Criminal Procedural and Technical Aspects Related to the Computer Search)*, in Dreptul (Law), issue no. 12/2014
14. Laura Codruta Kovesi, *Accesul si supravegherea sistemelor de telecomunicatii sau informatice. Mijloace de proba (Access and Surveillance of Telecommunications or Computer Systems. Means of Evidence)*, in Dreptul (Law), issue no. 7/2003
15. Simona Lungu, Mihaela Tilea, Dan Voinea, *Cercetarea la fata locului in cazul infractiunilor savarsite prin mijloace electronice (Crime Scene Investigation in the Case of Crimes Committed by Electronic Means)*, article published in the volume „Investigarea criminalistica a locului faptei" ("Crime Scene Forensic Investigation"), Asociatia Criminalistilor din Romania (Romanian Forensic Association), Ed. Luceafarul (Publishing House), Bucharest, 2004,
16. Rodica, Aida Popa, *Aspecte teoretice si practice referitoare la metodele speciale de supraveghere sau cercetare prevazute in Codul de procedura penala (Theoretical and Practical Aspects related to Special Surveillance or Investigation Methods Set Out in the Criminal Procedure Code)*, in Dreptul (Law), issue no. 6/2015