Bulletin of the *Transilvania* University of Braşov
Series VII: Social Sciences • Law • Vol. 14(63) Special Issue
https://doi.org/10.31926/but.ssl.2021.14.63.3.21

BRIEF CONSIDERATIONS REGARDING COMPUTER SEARCH

Camelia BOBASU[1]

Abstract: *Computer search is an evidence procedure that involves interfering with a person's private life; as a result, it must be disposed of only exceptionally. However, computer search should not be confused with access to a computer system, a process that involves entering a computer system or part of it or a means of storing computer data, either directly or remotely through specialized programs or through a network, in order to identify existing evidence or that generated during technical surveillance.*

Key words: *Data, computer search, search warrant.*

1. Introduction

The computer search finds its regulation in the current Criminal Procedure Code in chapter VI, entitled "*Searchand seizure of objects and documents"*, section II ("*Other forms of search*"), Art. 168-168 ind. 1 CPC.

The computer search can be ordered during the criminal investigation, by way of reasoned resolution, by the judge of rights and freedoms at the request of the prosecutor, and during the trial by the court, at the request of the prosecutor, of the injured person or ex officio; it will not be possible to order the computer search before the beginning of the criminal investigation or in the preliminary chamber procedure.

The settlement of the request takes place in the council chamber, without summoning the parties, with the mandatory participation of the prosecutor; the absence of the prosecutor in solving the request is sanctioned with absolute nullity under the conditions of Art. 281 (1) (a) of CPC.

Unlike the search of private property in which case the legislator established the cases and the conditions in which it is ordered, in the case of the computer search there is no such provision; from the corroboration of Art. 168 (2) final thesis CPC with the provisions of Art. 97 et seq. of the CPC it appears that the computer search will be ordered when, for the discovery and gathering of evidence, it is necessary to search for a computer system or a computer data storage medium.

[1] University of Craiova, cameliabobasu@yahoo.com, corresponding author

2. The Presence of the Lawyer during the Computer Search

According to Art. 92 (1) CPC, during the criminal investigation, the lawyer of the suspect or defendant has the right to assist in the carrying out of any act of criminal investigation, the exception to this rule being represented by the situation in which specific methods of surveillance are used or in case the investigation and body or vehicle search in flagrant offences are carried out.

The computer search does not fall within the exceptional situations listed in the Criminal Procedure Code, but there are no provisions referring to the presence of the lawyer in the case of computer search, as happens, for example, in the case of search of the private property where Art. 159 (9) CPC regulates the right of the person against whom the search of the private property is carried out to request the presence of a lawyer.

If the person against whom the search of the private property is carried out requests the presence of a lawyer, the start of the search is postponed until their arrival, but not more than two hours from the moment this right is communicated, taking measures to preserve the place to be searched (1) at the same time, and the searched person will be allowed to be assisted/represented by a reliable person.

The computer search is carried out in the presence of the suspect or defendant who will be informed that he/she has the right to be assisted by a lawyer during the computer search; in the event that the computer search took place without prior information of the suspect/defendant in connection with the presence of a lawyer, the sanction of absolute nullity is incident (Art. 281 (1)(e) and/or (f) NCPC, (Udroiu, 2019, p. 553); the nullity cannot be invoked in any stage of the process but only until the closing of the preliminary chamber procedure, if the violation occurred during the criminal investigation or until the closing of the preliminary chamber procedure.

If the suspect/defendant is detained or arrested, he/she will be brought to the search, and if he/she cannot be brought, the search in the computer system or of the computer data storage medium is carried out in the presence of a representative or an assistant witness, as it results from Art. 168 (1) corroborated with Art. 159 (11) CPC.

The provisions set forth by Art. 168 CPC refer only to the presence of the suspect/defendant in case of a computer search and there is no mention of the situation in which the computer search is performed on a computer medium that would belong to the injured person/civil party/civilly responsible party or a third party.

We consider that, in the event of a computer search on goods belonging to the categories of persons mentioned above, they may invoke the right to participate in person or through a representative (in the case of legal entities) in the computer search (Ciorea, 2017).

3. Execution of the Computer Search Warrant

In order to execute the ordered search, in order to ensure the integrity of the computer data stored on the seized objects, the prosecutor orders the making of copies; the copy will replace the original means of storing the computer data (Udroiu, 2019),

and the activity of gathering the samples within the computer search will be carried out by using software or specific hardware directly on the copy.

The computer search should not be confused with the technical-scientific finding which represents the means by which the knowledge of a specialist or technician is used, in the criminal investigation phase, for the urgent clarification of some facts or circumstances that require specialized knowledge; as a result, the object of the computer search cannot be the object of a technical-scientific finding.

The drafting of a technical-scientific finding report in which it is recorded the accomplishment of one of the activities specific to the computer search must lead to its requalification as a report of the computer search and, as a result, must comply with the conditions provided by Art. 168 CPC 9 (2) (Ciortea, 2017; Ionita, 2014).

The Criminal Procedure Code does not stipulate a time interval in which the warrant of computer search can be executed, unlike the old regulation which provided that the search, with two exceptions, must begin between 6 AM -20 PM, with the possibility to continue also during the night; as a result, the computer search will be carried out within the time period provided in the search warrant according to Art. 168 (6) (d) CPC.

In executing the search warrant, the criminal investigation bodies must take the necessary measures for this to be carried out without the facts and circumstances in the personal life of the person against whom the search is carried out becoming public, a principle that also emerges from the content of the Budapest Convention.

The result of the computer search will be written in a report that must include all the mentions provided by Art. 168 (13) CPC.

4. The Presence of the Specialist during the Computer Search

The search of the computer system or of a computer data storage medium is carried out by a specialist who works within the judicial bodies or outside them, in the presence of the prosecutor or of the criminal investigation body; by Art. 168 ind. 1 CPC introduced by GEO no. 18/2016 also provided the competence of specialized police officers to search the computer system or media for storing computer data.

The presence of the specialist in carrying out the computer search is also imposed in the jurisprudence of the ECHR; for example, in the case *Wieser and BicosBeteiligungen GmbH vs. Austria* it was considered that the participation of the specialist in only a part of the operations that this evidentiary procedure presupposed, contributed to the violation of the provisions of Art. 8 of the Convention.

5. Keeping Professional Secrecy

There are certain professional categories in respect of which a strict regulation of the guarantees compared to the common procedure is necessary, so that the professional secrecy is protected.

According to Art. 139 (4) CPC: "*the relationship between the lawyer and the person he/she assists or represents cannot be the object of technical surveillance unless there is data that the lawyer commits or prepares to commit an offence among those provided in*

par. 2", considered as serious offences. In addition, "*if during or after the execution of the measure it appears that the technical surveillance activities concerned also the relationship between the lawyer and the suspect or defendant he/she defends, the evidence obtained cannot be used in any criminal proceedings, and will be destroyed, immediately, by the prosecutor. The judge who ordered the measure is immediately informed by the prosecutor".*

Considering the legal texts mentioned above, it results that the relationship between the lawyer and the person he/she assists/represents cannot be the object of technical surveillance; however, regarding the computer search, there is no provision in the Criminal Procedure Code regarding the lawyer-suspect/defendant relationship.

6. Access to a Computer System

Computer search should not be confused with access to a computer system that involves entering a computer system or part of it (such as accessing email) or a means of storing computer data, either directly or remotely through specialized programs or through a network, in order to identify existing evidence or that generated during technical surveillance.

According to Art. 141 (5) CPC, in situations where there is urgency and obtaining the technical surveillance warrant under the conditions of Art. 140 CPC would lead to the delay of the investigations; the prosecutor has the right, when he/she has access to an information system, according to Art. 138 (1) (b) CPC, to order by ordinance the following:

- Making and preserving a copy of this computer data (copies are made with adequate technical and procedural means to ensure the integrity of the information contained therein).
- Suppression of accessing or removing this computer data from the computer system.

After carrying out these activities, the prosecutor is obliged to make a motivated request for obtaining the search warrant.

The computer search involves the information of the person in whose computer system the entering takes place, as well as his/her participation in the evidentiary procedure, as opposed to the access to a computer system that has a confidential character.

The computer search cannot be ordered before the beginning of the criminal investigation or in the preliminary chamber procedure; during the criminal investigation, the competence to order the computer search belongs to the judge of rights and freedoms from the court which would have the competence to judge the case in the first instance or from the corresponding court in its degree in whose district the prosecutor's office who conducts or supervises the criminal investigation is located.

Regarding the computer search, this evidentiary procedure is used to obtain computer data represented by the content of email or SMS messages, provided that they are already stored on the computer medium to be searched and in the custody of the judicial body.

While the computer search is used to obtain already existing computer data, located in a computer system already in the custody of the judicial body, in the case of computer data represented by the content of email or SMS messages stored on computer systems that are not in the custody of the judicial body, the evidentiary hearing by which this data can be obtained is represented by the access to a computer system.

Therefore, in this last situation it is necessary to issue a warrant for computer search by the judge of rights and freedoms.

The difference between a computer search and access to a computer system is given by the fact that, in the case of a computer search, the computer data is that which already exists on the computer system searched, thus being data from the past at the date of the issuance of the computer search warrant, as opposed to access to a computer system in which case it is possible to obtain data on communications made prior to the date of issuance of the technical surveillance warrant.

In many cases, during computer searches, the contents of emails, messages or other types of communications transmitted, received or archived from that computer system or from another computer system are identified in the form of computer data.

It is clear that in the case of such pre-existing IT data, even if it is data concerning the content of communications, it is not necessary to request the issuance of a technical supervision warrant consisting in intercepting communications already made or authorizing access to an IT system.

To consider as unlawful the obtaining of computer data represented by the content of email or VoIP messages by means of a computer search and to validate as lawfully obtained such data only when it has been obtained by the method of interception or access to a computer system would mean that, under such an interpretation, no communication of any kind which is useful for the resolution of the case and the finding of the truth and which has already been transmitted/received could be used in the criminal investigation.

However, this was not the intention of the legislator when adopting criminal procedural measures necessary to obtain and use computer evidence in criminal investigations and adapted to the realities of the 21st century.

While computer search is used to obtain existing computer data located in a computer system already in the custody and under the control of the judicial body, in the case of computer data represented by the content of email or VoIP messages stored on computer systems not in the possession of the judicial body, the evidentiary procedure through which this data can be obtained is represented by the access to a computer system.

Also, in this situation it is necessary to issue a warrant by the judge of rights and freedoms, the data being obtained with the help of specific technical means, with or without the support of Internet service providers or communications.

What further distinguishes access to a computer system from a computer search is that, whereas in the case of a computer search, the computer data is that already existing in the computer system searched, i.e. data from the past at the time the computer search warrant was issued, access to a computer system can obtain data on communications prior to the date of issue of the technical supervision warrant, as well

as data on subsequent communications made between the time the warrant was issued and the deadline by which it is valid.

With regard to these communications after the date of issuance of the supervision warrant, again, this method of obtaining data should not be considered as interception of data, because even if access to the computer system may result in some computer data being obtained immediately after receipt or transmission, this aspect cannot be equivalent to interception.

As stated above, the interception takes place between the moment of transmission of the communication and the moment of receipt of the communication, whereas in the case of access to a computer system, the obtaining of data on the content of the communication takes place after the end of the communication chain.

The specialized literature analyzed the procedural sanction that intervenes in the case of performing specific activities of computer search in the absence of a computer search warrant, but with the consent of the user of the computer system or the means of storing computer data.

It has been shown that such a situation is, in fact, a breach of functional competence, as long as the search of the computer can be ordered only by the judge of rights and freedoms or by the court.

Thus, in consideration of this thesis, the procedural sanction that intervenes is the absolute nullity (Udroiu, Zlati, 2015, pp. 857-858)

7. Conclusion

Considering that both the computer search and the access to a computer system imply the interference in the private life of a person, *de lege ferenda* we appreciate that it is necessary to improve the provisions regarding these procedures, on the one hand to achieve a better delimitation between them, and on the other hand, by regulating several guarantees for the protection of the persons concerned by these evidentiary procedures.

References

Ciorea, P. (2017). Brief considerantion regarding computer search. *Revista Penalmente/Relevant, Nr. 1*. Retrieved from Paula-CIOREA- Brief Consideration regarding computer search .pdf (penalmente.ro)

Ionita, G.I. (2014). Procedural criminal and technicall isuess regarding computer search. *Law* nr. 12/2014

Udroiu, M., Zlati, G. (2015). *Codul de procedură penală. Comentarii pe articole* [Criminal Procedure. Comments on articles], Second Edition. Bucharest: C.H. Beck.

Udroiu, M. (2019). *Procedură penală. Partea Generală* [Penal procedure. General part.] Bucharest: Publishing House C.H. Beck.