EUROPEAN JUDICIAL NETWORK

# Fiches Belges on electronic evidence

## ROMANIA

1. Definition of electronic evidence

Art. 97 of the Criminal Procedure Code provides that "*any factual element serving to the ascertaining of the existence or non-existence of an offense, to the identification of a person who committed such offense and to the knowledge of the circumstances necessary to a just settlement of a case, and which contribute to the finding of the truth in criminal proceedings represents evidence*".

Thus, the evidence is obtained in criminal proceedings through means of prove and objects of evidence and is presented through the methods of prove provided by law.

Romanian legislation does not provide for a definition of electronic evidence, however, practice admits that the "**electronic evidence**" (digital evidence) represents ***any factual element, created or existing in an electronic (digital) medium serving to the ascertaining of the existence or non-existence of an offense, to the identification of a person who committed such offense and to the knowledge of the circumstances necessary to a just settlement of a case.***

Computer search is a method of obtaining/retrieving electronic evidence in a criminal proceeding, a case of cybercrime or any other case in which it is necessary to collect electronic evidence. The Romanian Criminal Procedure Code sets up the legal framework for conducting a computer search. to

With regard to production of evidence, including electronic evidence, as a general rule, the provisions of Article 100 of the Criminal Procedure Code provides that during the criminal investigation, investigation bodies gather and produce evidence both in favour and against a suspect or a defendant, ex officio or upon request, and, during the trial, this role belongs to the court, who produces evidence upon request by the prosecutor, the victim or the parties and, ex officio, when it deems it necessary for the settlement of its own conviction.

The above-mentioned article establishes the main characteristics of the evidence, i.e. a piece of evidence should be relevant to the object of evidentiary in a case, as stipulated under Art. 98 of the Criminal Procedure Code. Also, the evidence must be necessary and useful, i.e. it is not meant to prove a fact of notoriety, or not sufficient evidence has been produced for proving a factual element representing the object of evidentiary, the piece of evidence is not impossible to obtain, the production of evidence is legal and was requested by a person who has such right.

In deciding the existence of an offense and on a defendant's guilt, the court decides, on a justified basis, on the basis of all the assessed pieces of evidence. Conviction is ordered only when the court is convinced that the charge was proven beyond any reasonable doubt.

Art.197 para.1 and 2 of the Criminal Procedure Code stipulates that objects containing or bearing traces of a committed offense are physical evidence (for example HDD, CD, DVD, router, memory stick

or any other piece of equipment and the objects used to the commission of an offense are *corpus delicti* (for example the computer system used).

Considering the particular nature of the evidence that is produced, transmitted or kept in a computer system, the Criminal Procedure Code has established special rules on how the electronic surveillance is performed, how computer search is carried out, and how computer data are surrendered or preserved.

2. Which measures are possible in your Member State under International Judicial Cooperation?

- special methods of surveillance or investigation *see answer to 3.a.i;
- computer search *see answer to 3.a.v;
- production orders (surrender of objects, documents or computer data) *see answer to 3.a.iii;
- preservation of computer data (includes data content, traffic data or subscriber information *see answer to 3.a.iv. and expedited disclosure of traffic data (implementation of Art.29-30 of the Budapest Convention)

3. Procedure for obtaining electronic evidence
   a. National procedures

i. **The Criminal Procedure Code establishes under Chapter IV Art. 138 the following special methods of surveillance or investigation:**

- **wiretapping of communications or of any type of remote communication;**
- **accessing a computer system;**
- video, audio or photo surveillance;
- tracking or tracing with the use of technical devices;
- obtaining data regarding the financial transactions of individuals;
- withholding, delivery or search of mail deliveries;
- use of undercover investigators and informants;
- authorized participation in specific activities;
- controlled delivery;
- **obtaining traffic and location data processed by providers of public electronic communication networks or by providers of electronic communication services intended for the public.**

According to Art. 139 RCPC electronic surveillance may be ordered in case of offenses against national security stipulated by the Criminal Code and by special laws, as well as in case of drug trafficking, weapons trafficking, trafficking in human beings, acts of terrorism, money laundering, counterfeiting of currency or securities, counterfeiting electronic payment instruments, offenses against property, blackmail, rape, deprivation of freedom, tax evasion, corruption offenses and offenses assimilated to corruption, offenses against the European Union's financial interests, **offenses committed by means of computer systems or electronic communication devices**, or in case of other offenses in respect of which the law sets forth a penalty of no less than 5 years of imprisonment.

Pursuant to Art.140 RCPC electronic surveillance may be ordered during the criminal investigation, for a term of maximum 30 days, upon request by the prosecutor, the Judge for Rights and Liberties of the court having jurisdiction to examine the case in first instance or of the court corresponding to its level

under whose territorial jurisdiction the premises of the prosecutors' office to which the prosecutor who filed the application belongs are located. If they decide that the application is justified, the Judge for Rights and Liberties shall order admission of the prosecutor's application, through a court resolution, and shall issue forthwith an electronic surveillance warrant.

Upon reasoned request by the victim, the prosecutor may request the judge to authorise wiretapping or recording of communications, as well as any type of communication performed by the person concerned via any means of communication, irrespective of the nature of the offense that is subject to investigation.

Art. 141 RCPC provides for the situations in which the prosecutor may authorise for a period of maximum 48 hours, electronic surveillance measures, under the obligation to notify the Judge for Rights and Liberties within a maximum of 24 hours following expiry of a measure and forward a report presenting a summary of the electronic surveillance activities performed and the case file.

In respect of computer data identified through accessing a computer system, the prosecutor may order, through a prosecutorial order:

- making and preservation of a copy of such computer data;
- prohibition of access to or removal of such computer data from the computer system.

Copies shall be made by means of appropriate technical devices and procedures, of nature to ensure the integrity of information contained by these.

The electronic surveillance warrant may be extended, for well-grounded reasons, by the Judge for Rights and Liberties of the court of competent jurisdiction, upon reasoned request by the prosecutor, in situations where certain requirements are met; however, each such extension may not exceed 30 days.

Following the termination of an electronic surveillance measure, the prosecutor shall inform each subject of the warrant for electronic surveillance enforced against them, in writing, within maximum 10 days (Art. 145 RCPC).

ii. **Art.152 - Obtaining data generated or processed by providers of public electronic communications networks or providers of electronic communication services intended for the public**

Criminal investigation bodies, subject to a prior authorization from the Judge for Rights and Liberties, may request a provider of public electronic communication networks or a provider of electronic communication services intended for the public to transmit the traffic or location data if the following cumulative conditions are fulfilled as such:

- there is a reasonable suspicion in relation to the commission of an offense provided by Article 139 para. (2) or of an offense of disloyal competition, escape, counterfeiting documents, non-compliance with the rules governing weapons, ammunition, nuclear material and explosives, non-compliance with the rules governing introducing in the country waste and residues, an offence regarding organising and exploiting gambling or an offence related to drug precursors and offences related to operations with products with psychoactive effects similar to narcotic and psychotropic substances;
- there are grounds to believe that the requested data represent evidence;
- evidence could not be obtained in any other way or its obtaining implies special difficulties that would harm the investigation, or there is a threat for the safety of persons or of valuable goods;

- the measure is proportional to the restriction of fundamental rights and freedoms, considering the particularities of the case, the importance of information or evidence that are to be obtained or the seriousness of the offense;

The Judge for Rights and Liberties shall rule within 48 hours on requests transmitted by criminal investigation bodies regarding the transmission of data, through a reasoned court resolution, in chambers. Providers of public electronic communication networks and providers of electronic communication services intended for the public that cooperate with criminal investigation bodies are under an obligation to keep secrecy of the conducted operations.

iii. **Preservation of computer data (Art. 154 RCPC)**

If there is a reasonable suspicion in relation to the preparation or commission of an offense, for the purpose of collecting evidence or of identifying a perpetrator, suspect or defendant, the prosecutor supervising or conducting the criminal investigation may order immediate preservation of computer data, including of data referring to information traffic, that were stored by means of a computer system and that is in the possession or under the control of a provider of public electronic communication networks or of a provider of electronic communication services intended for the public, in the event that there is a danger that such data may be lost or altered.

The preservation is ordered by the prosecutor, ex officio or upon request by criminal investigation bodies, for a term of maximum 60 days, through an order that has to contain besides the obligations provided by Article 286 paragraph (2): the providers of public electronic communication networks or the providers of electronic communication services intended for the public in which possession or control the computer data is, the name of the perpetrator, suspect or defended if known, a description of the data to be preserved, justification of the fulfilment of the conditions required by paragraph 1, the duration for which it was issued, a mention of the obligation of the person or providers of public electronic communication networks or the providers of electronic communication services intended to immediately preserve the indicated computer data and maintain the data integrity, under conditions of confidentiality.

The preservation measure may be extended by the prosecutor, only once, for well-grounded reasons, for a term of maximum 30 days.

The prosecutor's order is transmitted immediately to any provider of public electronic communication networks or provider of electronic communication services intended for the public holding the data specified under paragraph (1) or having control on such data, the latter being under the obligation to preserve it immediately, under confidentiality terms.

If data referring to information traffic is held by several providers of public electronic communication networks or providers of electronic communication services intended for the public, a provider holding or controlling the computer data is under an obligation to provide the criminal investigation bodies forthwith with the information necessary for the identification of other providers, in order to enable them to learn of all elements of the used communication chain.

The prosecutor supervising or conducting the criminal investigation, based on a prior authorisation from the Judge for Rights and Liberties, may request a provider of public electronic communication networks or a provider of electronic communication services intended for the public to transmit the data preserved under the law or may order cancellation of such measure.

The Judge for Rights and Liberties shall rule on requests transmitted by criminal investigation bodies regarding the transmission of data within 48 hours, through a reasoned court resolution, in chambers.

These provisions apply accordingly to computer data, including traffic data stored through computer systems held or under control of other persons.

Before completion of the criminal investigation, the prosecutor is under an obligation to inform in writing the persons against whom the criminal investigation is conducted and whose data were preserved.

iv. **ART. 170 RCPC - Surrender of objects, documents or computer data**

In the event that there is a reasonable suspicion in relation to the preparation or commission of an offense and there are reasons to believe that an object or document can serve as evidence in a case, the criminal investigation bodies or the court may order the natural person or legal entity holding them to provide and surrender them, subject to receiving proof of surrender.
(Also, under the same terms criminal investigation bodies or the court may order:

- any natural person or legal entity on the territory of Romania to communicate specific computer data in their possession or under their control that is stored in a computer system or on a computer data storage medium;
- any provider of public electronic communication networks or provider of electronic communication services intended for the public to communicate specific data referring to subscribers, users and to the provided services that is in its possession or under its control, other than the content of communications and then those that nay be retrieved under art.152 RCPC.

Natural persons or legal entities, including providers of public electronic communication networks or providers of electronic communication services intended for the public, can ensure the signing of the data requested by using an extended electronic signature based on a qualified certificate issued by an accredited certification service provider.

Any authorized person transmitting data requested can sign the transmitted data by using an extended electronic signature based on a qualified certificate issued by an accredited certification service provider, and which allows for an unambiguous identification of the authorized person, thus taking responsibility for the integrity of the transmitted data.

Any authorized person receiving such data can check the integrity of the received data and certify such integrity by signing them, by means of an extended electronic signature based on a qualified certificate issued by an accredited certification service provider, and which allows for an unambiguous identification of the authorized person.

Each person certifying data based on an electronic signature shall be liable for the integrity and security of such data under the law.

v. **Art. 168 RCPC– Computer search**

A computer system search or a computer data storage medium search designates the procedure for the investigation, discovery, identification and collection of evidence stored in a computer system or in a computer data storage medium, performed by means of adequate technical devices and procedures, of nature to ensure the integrity of the information contained by these.

During a the criminal investigation, the Judge for Rights and Liberties of the court that would have the competence of jurisdiction to examine the case in first instance or of the court corresponding to its level under whose territorial jurisdiction the premises of the prosecutors' office with which the prosecutor conducting or supervising the criminal investigation is working are located may order the conducting of a computer search, upon request by the prosecutor, when the investigation of a computer system or of a computer data storage medium is necessary for the discovery and collection of evidence.

The prosecutor shall apply requesting the approval of a computer search together with the case file to the Judge for Rights and Liberties. Such application is ruled on in chambers, without summoning the parties. The prosecutor's attendance is mandatory.

The judge orders, through a court resolution, to sustain the application, when this is well-grounded, to approve the computer search, and issues a search warrant forthwith.
The court resolution through which the Judge for Rights and Liberties decides upon an application for the approval of a computer search is not subject to avenues of appeal.

In the event that, on the occasion of a search of a computer system or of a computer data storage medium, it is found that the sought computer data is stored in a different computer system or a computer data storage medium, and is accessible from the initial system or medium, the prosecutor shall immediately order the preservation and copying of the identified computer data and shall request the issuance of a warrant on an emergency basis. The general stipulations apply accordingly.

In conducting the ordered search, in order to ensure integrity of the computer data stored on the seized objects, the prosecutor shall order the making of copies of them.

If the seizure of objects containing computer data subject to a computer search seriously hinders the activities of the persons holding such objects, the prosecutor may order to copy them and the copies would serve as methods of proof. Copies are made with adequate technical devices and procedures, of nature to ensure the integrity of the information contained by these.

The computer system or computer data storage medium search is conducted in the presence of a suspect or a defendant, general stipulation regarding his presence to a home search would apply accordingly.

A computer system or computer data storage medium search is conducted by a specialist working with the judicial bodies or an external one, in the presence of the prosecutor or of the criminal investigation bodies, or by a specialized police officer.

Criminal investigation bodies have to make sure that the search is conducted without making facts and circumstances of the private life of the person subject to search public in an unjustified manner. Computer data of a secret nature identified during such search is kept under the law.

During the trial, computer search is ordered by the court, ex officio or upon request by the prosecutor, by the parties or the victim. A warrant for a computer search ordered by the court shall be communicated to the prosecutor, who shall act accordingly.

b. international procedures (including Available channels/ways to obtain electronic evidence from your Member State; urgent procedures; specialised networks to obtain electronic evidence e.g. 24/7 Budapest Convention/police channels)

Any of the above-mentioned provisions may be subject of an international cooperation request. In the Romanian legislation there is no special procedure for emergency situations. However, requests stating an emergency are treated immediately with due diligence.

4. International legal framework applicable for this measure in your Member State

- EIO
- EU MLA Treaty + Protocol
- MLA CoE Convention + Protocol
- UNTOC
- Budapest Convention – Chapter III

5. competent authority to receive and execute your request

The competent authority, depending on the stage of the investigation, trial and the type of the request is set forth by Law no 302/2004 (amended)

For the list of competent authorities see:

http://www.ejncrimjust.europa.eu/ejn/libdocumentproperties.aspx?Id=331

A special procedure is provided for preservation requests which are sent and received according to the provisions of the Law no.161.2003 – Title III, Chapter V.

Art. 63

(1) Within the international cooperation, the competent foreign authorities can require from the Service for combating cybercrime the expeditious preservation of the computer data or of the data regarding the traffic data existing within a computer system on the territory of Romania, related to which the foreign authority is to formulate a request of international legal assistance in criminal matters.

(2) The request for expeditious preservation referred to at paragraph (1) includes the following:
   a) the authority requesting the preservation;
   b) a brief presentation of facts that are subject to the criminal investigation and their legal background;
   c) computer data required to be preserved;
   d) any available information, necessary for the identification of the owner of the computer data and the location of the computer system;
   e) the utility of the computer data and the necessity to preserve them;
   f) the intention of the foreign authority to formulate a request of international legal assistance in criminal matters;

(3) The preservation request is executed according to art. 54 for a period of 60 days at the least and is valid until a decision is taken by the Romanian competent authorities, regarding the request of international legal assistance in criminal matters;

6. accepted languages

RO, EN, FR

7. Definition of data category and examples: subscriber, traffic/transaction and content data in terms of requirements and thresholds for access to data needed in specific criminal investigations

**Definitions derived from the Budapest Convention are provided by Art. 35 of Law No. 161/2003, as following:**

- **computer system** means any device or combination of interconnected devices or in a functional relation, one or more of which, pursuant to a program, performs automatic processing of data;
- **automatic data processing** means the process by which data from a computer system are processed through a computer program;
- **computer program** means a set of instructions that can be performed by a computer system to achieve a specific result;
- **computer data** means any representation of facts, information or concepts in a form that can be processed by a computer system. This category includes any computer program that can determine performance of a function by a computer system;
- **data on traffic information** means any computer data related to a communication made via a computer system and its products, which is part of the communication chain, indicating the origin, destination, route, time, date, size, volume and duration, and type of service used for communication;
- **user data** means any information that may lead to the identification of a user, including type of communication and service used, address, geographical, phone numbers or any other access numbers and manner of payment of that service, and any other data that may lead to identification of the user.

Other definitions are stipulated in the Criminal Procedure Code in Art.138 para.(4) and (5):

- computer system means any device or combination of interconnected devices or in a functional relation, one or more of which, pursuant to a program, performs automatic processing of data;
- computer data mean any representation of facts, information or concepts in a form appropriated for processing in a computer system, including a program able to determine the performance of a function by a computer system.

8. Voluntary-disclosure:
   a. As issuing state: Admissibility of the electronic evidence obtained by voluntary disclosure.

If data is obtained via voluntary disclosure from a foreign ISP, it may be treated as information.

   b. As executing state: Procedures/legislation in your Member State with regards to the possibility for the OSPs in your Member State to provide data directly to other Member States

Romanian legislation does not contain any provision related to voluntarily disclosure. Romanian ISP do not respond to such requests.

9. Data retention periods (including procedures for extensions)

Romanian legislation does not contain any provision related to mandatory data retention.

10. Procedure for data preservation/execution deadline

*See answer to 3.a.iv

EUROPEAN JUDICIAL NETWORK

11. Procedure for data production/ execution deadline

*See answer to 3.a.iii

12. Concise legal practical information