BILAG 4



MINISTERUL JUSTITIEF

Bucharest 25 September 2015 Our ref. 75864/2015 Your ref. 2015-42343/861082

#### Royal Danish Embassy Bucharest

The Ministry of Justice of Romania presents its regards to the Royal Danish Embassy and, referring to the note verbale from 16 September 2015, has the honour to transmit, attached, an excerpt from the Romanian code of criminal proceedings, concerning the legal provisions applicable when issuing a search warrant and authorizing phone tapping.

The Ministry of Justice of Romania avails itself of this occasion to renew to the Royal Danish Embassy the assurance of its highest consideration.  $\mathcal{M}$ 



SB. Anoladoi m. 17. сероя 5. (19174). Высшелеть Власт Теї +4.037.212 ток.

Pagina 1 din 1 7 7 80 ES rel dif vez 2

#### <u>CHAPTER IV</u> Surveillance or investigation special methods

#### <u>ART. 138</u>

.

#### **General provisions**

(1) The following are surveillance or investigation special methods:

a) wiretapping of communications or of any type of remote communication;

b) accessing a computer system;

c) video, audio or photo surveillance;

d) tracking or tracing with the use of technical devices;

e) obtaining data regarding the financial transactions of individuals;

f) withholding, delivery or search of mail deliveries;

g) use of undercover investigators and informants;

h) authorized participation in specific activities;

i) controlled delivery;

j) obtaining data generated or processed by providers of public electronic communication networks or by providers of electronic communication services intended for the public, other than the content of communications, stored by these under the special law on storing data generated or processed by providers of public electronic communication networks and by providers of electronic communication services intended for the public.

(2) Wiretapping of communications or of any type of messages designates the wiretapping, accessing, monitoring, collection or recording of communications via phone, computer system or any other communication device.

(3) Accessing a computer system designates the penetration of a computer system or of other data storage device either directly or from a distance, through specialized programs or through a network, for the purpose of identifying evidence.

(4) A computer system is any device or combination of devices interconnected between them or in a functional relationship, one or more of which provide the automatic data processing by means of a computer program.

(5) Computer data is 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.

(6) Video, audio or photo surveillance is the taking of pictures of persons, the observation or recording of their conversations, gestures or other activities.

(7) Tracking or tracing with the use of technical devices is the use of devices that establish the location of the person or the object to which such devices are attached.

(8) Search of mail deliveries designates the inspection, through physical or technical methods, of letters or other mail deliveries or objects transmitted through any other means.

(9) Obtaining of data regarding the financial transactions of individuals designates operations that provide knowledge of the contents of financial transactions and other operations performed or to be performed through a credit institution or through other financial entity, as well as the obtaining from a credit institution or other financial entities of documents or information held by it referring to the transactions or operations of a person.

(10) Use of undercover investigators and informants designates the use of a person with an identity other than their real one, for the purpose of obtaining data and information regarding the commission of an offense.

(11) Authorized participation in specific activities means the commission of acts similar to the objective component of a corruption offense, the performance of transactions, operations or any other kind of arrangements related to an asset or to a person who is presumed missing, a victim of trafficking in human beings or of kidnapping, the performance of operations involving drugs, as well as the providing of services, based on an authorization from the judicial bodies of competent jurisdiction for the purpose of obtaining evidence.

(12) Controlled delivery designates a surveillance and investigation technique allowing for the entry, transit or exit from the territory of the country of goods in respect of which there is a suspicion related to the illicit nature of their possession or obtaining, under the surveillance of or based on an authorization from the competent authorities, for the purpose of investigating an offense or of identifying the persons involved in its commission.

(13) Electronic surveillance is the use of any of the methods listed under par. (1) items a) - c).

#### <u>ART. 139</u>

•

#### Electronic surveillance

(1) Electronic surveillance is ordered by the Judge for Rights and Liberties when the following requirements are cumulatively met:

a) there is a reasonable suspicion in relation to the preparation or commission of one of the offenses listed under par. (2);

b) such 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; c) 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.

(2) 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.

(3) The recordings set forth by this chapter, done by the parties or by other persons, represent evidence when they concern their own conversations or communications with third parties. Any other recordings may constitute evidence unless prohibited by law.

(4) The relationship between a counsel and a person assisted or represented by them may be subject to electronic surveillance only when there is information that the counsel perpetrates or prepares the commission of any of the offenses listed under par.(2). If during or after the performance of such measure it results that the activities of electronic surveillance also targeted the relations between the counsel and the suspect or defendant defended by the former, the evidence obtained this way may not be used in a criminal proceeding, and shall be destroyed forthwith by the prosecutor. The judge having ordered such measure shall be informed forthwith by the prosecutor. When deemed necessary, the judge may order the information of the counsel.

#### <u>ART. 140</u>

.

#### Procedure for the issuance of an electronic surveillance warrant

(1) 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 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 to which the prosecutor who filed the application belongs are located.

(2) Such application filed by the prosecutor has to contain: the electronic surveillance measures that are requested for authorization, the name or the identification data of the person against whom such measure is to be ordered, if known, the evidence or data giving rise to a reasonable suspicion related to the commission of an offense in respect of which such measure may be ordered, the facts and the charges, and, in case of a video, audio or photo surveillance measure, whether an approval for criminal investigation bodies to enter private spaces

indicated for activating and deactivating the technical devices to be used for the enforcement of the electronic surveillance measure is also requested, and a justification of the proportional and subsidiary nature of the measure. The prosecutor has to submit the case file to the Judge for Rights and Liberties.

(3) An application requesting approval of electronic surveillance shall be ruled on in chambers, on the same day, without summoning the parties. The prosecutor's attendance is mandatory.

(4) 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 a electronic surveillance warrant. Writing of a report is mandatory.

(5) The court resolution of the Judge for Rights and Liberties and the warrant have to contain:

a) name of the court;

b) warrant issuance date, time and venue;

c) surname, first name and capacity of the person returning the court resolution and issuing the warrant;

d) description of the concrete approved measure;

e) time period and purpose for which the measure was authorized;

f) name of the person subject to a electronic surveillance measure or their identification data, if known;

g) indication, if necessary given the nature of the approved measure, of the identification elements of each phone device, of the access point to a computer system, and of any known data for the identification of a communication channel or of an account number;

h) in case of a measure of video, audio or photo surveillance in private spaces, mention of approving permission to criminal investigation bodies to enter private spaces in order to activate and deactivate the technical devices to be used for the enforcement of the electronic surveillance measure;

i) signature of the judge and stamp of the court.

(6) In the event that the Judge for Rights and Liberties decides that the requirements set by <u>Art. 139</u> and The stipulations of par. (1) of this Article are not met, they shall deny the application for approving a electronic surveillance measure, through a court resolution.

(7) A court resolution under which the Judge for Rights and Liberties rules on electronic surveillance measures is not subject to avenues of appeal.

(8) A new application for the approval of the same measure may be filed only if new facts or circumstances, which were not known at the moment when the Judge for Rights and Liberties ruled on the previous application, occurred or were discovered.

(9) Upon justified request by an victim, the prosecutor may request the judge to authorize the wiretapping or recording of communications, as well as of any types of communications performed by them through any communication device, irrespective of the nature of the offense subject to investigation. The stipulations of par. (1) - (8) shall apply accordingly.

#### ART. 141

# Authorization of electronic surveillance measures by the prosecutor

(1) The prosecutor may authorize, for a time period of maximum 48 hours, electronic surveillance measures when:

a) there is an emergency situation, and the obtaining of a electronic surveillance warrant under the terms of <u>Art. 140</u> would lead to a substantial delay of investigations, to the loss, alteration or destruction of evidence, or would jeopardize the safety of the victim, of witnesses or of their family members; and b) the requirements set by <u>Art. 139</u> par. (1) and (2) are met.

(2) A prosecutorial order authorizing electronic surveillance measures has to contain the mentions specified by <u>Art. 140</u> par. (5).

(3) Within a maximum of 24 hours following expiry of a measure, the prosecutor is under an obligation to notify the Judge for Rights and Liberties of the court having 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 to which the prosecutor who issued the order belongs are located, in order for them to confirm the measure and, at the same time, shall forward a report presenting a summary of the electronic surveillance activities performed and the case file.

(4) If the Judge for Rights and Liberties decides that the requirements set by par. (1) were met, they shall confirm the measure ordered by the prosecutor within 24 hours, through a court resolution, returned in chambers, without summoning the parties.

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

a) making and preservation of a copy of such computer data;

b) 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.

(6) If the Judge for Rights and Liberties decides that the requirements set by par. (1) were not met, they shall nullify the measure taken by the prosecutor and shall order destruction of the evidence thus obtained. The prosecutor shall destroy the evidence obtained this way and shall prepare a report in this sense.

(7) Together with the application for a confirmation of their measure, or separately, the prosecutor may request the Judge for Rights and Liberties to warrant electronic surveillance measures under the terms of <u>Art. 140</u>.

(8) A court resolution through which the Judge for Rights and Liberties rules on the measures ordered by the prosecutor is not subject to avenues of appeal.

#### <u>ART. 142</u>

# Enforcement of electronic surveillance warrants

(1) The prosecutor shall enforce an electronic surveillance measure or may order that this be enforced by criminal investigation bodies or by specialized employees of the law enforcement bodies or of other specialist bodies of the state.

(2) Providers of public electronic communication networks or providers of electronic communication services intended for the public or of communication or financial services are under an obligation to cooperate with the criminal investigation bodies, the authorities listed under par. (1), within the limits of their authority, for the enforcement of electronic surveillance warrants.

(3) Persons who are called to provide technical support for the enforcement of surveillance measures are under an obligation to keep secrecy in respect of the performed operation, under penalties set by the criminal law.

(4) The prosecutor is under an obligation to cease electronic surveillance forthwith before expiry of the warrant term if the reasons justifying such measure no longer exist, by immediately informing the judge having issued the warrant.

(5) Data resulted from electronic surveillance measures may be used also in other criminal case if they contain eloquent and useful data or information regarding the preparation or commission of another crime of those set forth by Art. 139 par. (2).

(6) Data resulted from surveillance measures that do not concern the act subject to investigation or that do not contribute to the identification or locating of persons, if such are not used in other criminal cases as per par. (5), shall be archived at the premises of the prosecutors' office, in special places, by ensuring their confidentiality. Ex officio or upon request by the parties, the vested judge or judicial panel may request the sealed data if there is new evidence from which it results that part of these concern an act subject to investigation. One year after the final settlement of a case, these are destroyed by the prosecutor, who shall prepare a report in this sense.

#### <u>ART. 142^1</u>

(1) Any authorized person conducting electronic surveillance activities, under this law, has the possibility to ensure the electronic signing of data resulting from

electronic surveillance activities, by using an extended electronic signature based on a qualified certificate issued by an accredited certification services provider.

(2) Any authorized person who transmits data resulting from electronic surveillance activities under this law, has the possibility to sign the transmitted data by using an extended electronic signature based on a qualified certificate issued by an accredited certification services provider, which allows for the unambiguous identification of the authorized person, the latter taking this way responsibility for the integrity of the transmitted data.

(3) Any authorized person who receives data resulting from electronic surveillance activities under this law, has the possibility to check the integrity of the received data and to certify such integrity by signing them by means of an extended electronic signature based on a qualified certificate issued by an accredited certification services provider, which allows for the unambiguous identification of the authorized person.

(4) Each person certifying data under electronic signature is liable for the security and integrity of such data under the law.

#### <u>ART. 143</u>

# **Recording of electronic surveillance activities**

(1) Prosecutors or criminal investigation bodies shall prepare a report for each electronic surveillance activity, in which they shall record the results of activities conducted in respect of an act subject to investigation or that contribute to the identification or localization of persons, the identification data of the medium containing the results of electronic surveillance activities, the names of persons to whom these refer, if known, or other identification data, as well as, as applicable, the date and time when such electronic surveillance activity started and the date and time when it ended.

(2) A copy of the medium containing the results of electronic surveillance activities shall be attached to the reports, in a sealed envelope. Such medium or a certified copy of it shall be kept at the premises of the prosecutors' office, in special places, in a sealed envelope, and shall be made available to the court upon request. Following seizure of the court, a copy of the medium containing electronic surveillance activities and copies of the reports shall be kept at the court's registry office, in special places, in a sealed envelope, at the exclusive disposal of the judge or judicial panel vested with the case disposition.

(2<sup>1</sup>) Any authorized person making copies of a computer data storage medium containing results of electronic surveillance activities has the possibility to check the integrity of the data included in the original medium and, after making a copy, to sign the data included in it, by means of an extended electronic signature based on a qualified certificate issued by an accredited certification services provider, which

allows for the unequivocal identification of the authorized person, the latter taking this way responsibility for the integrity of data.

والمراجعة والمراجعة والمراجعة والمراجعة والمراجع والمراجع والمراجع والمراجعة والمراجعة والمراجعة والمراجع والمراجع

الممرور المراكب المتمرك المراكبين المراجع ومرجع مستمر مترجع والمراجع مراجع والمراجع والمراجع

------

(3) Phone conversations, communications or discussions in a language other than Romanian shall be transcribed in Romanian, by means of an interpreter, who is under an obligation to keep their confidentiality.

(4) Wiretapped and recorded phone conversations, communications or discussions concerning an act subject to investigation or which contribute to the identification or localization of persons, shall be transcribed by the prosecutor or the criminal investigation bodies in a report that shall mention the warrant issued for their conducting, the phone numbers, the identification data of computer systems or of access points, names of the persons who made such communications, if known, and the date and time of each conversation or communication. Such report shall be certified by the prosecutor for authenticity purposes.

(5) After termination of a surveillance measure, the prosecutor shall inform the Judge for Rights and Liberties on the performed activities.

#### <u>ART. 144</u>

.

# Extension of an electronic surveillance warrant

(1) An 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 the requirements set by <u>Art.</u> 139 are met; however, each such extension may not exceed 30 days.

(2) The Judge for Rights and Liberties shall rule in chambers, without summoning the parties, through a court resolution that is not subject to avenues of appeal. Preparation of a session minutes shall be mandatory.

(3) The total duration of an electronic surveillance measure, related to the same person and the same act, may not exceed, in the same case, 6 months, except for the measure of video, audio or photo surveillance in private spaces, which may not exceed 120 days.

#### ART. 145

# Information of persons subject to surveillance

"ATT TO A THE POST A COMMENCE AND A THE MEAN AND A POST AS A STATE OF A S

(1) Following 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.

(2) Following such information, a person subject to surveillance has the right to learn, upon request, of the content of the minutes recording the electronic surveillance activities performed. Also, the prosecutor has to ensure, upon request, the listening to discussions, communications or conversations, or the watching of images resulted from each electronic surveillance activity. (3) The term for filing a request in this sense is of 20 days as of the date of communication of the written information set under par. (1).

(4) The prosecutor may postpone such information or the presentation of media on which electronic surveillance activities are stored or the minutes transcribing them, in a justified way, if this could result in:

a) disruption or jeopardizing of the proper conducting of the criminal investigation in the case;

b) jeopardizing of the safety of the victim, witnesses or members of their families;

c) difficulties in the electronic surveillance of other persons involved in the case. (5) The postponement set under par. (4) may be ordered until completion of the criminal investigation or until the case closure, at the latest.

#### <u>ART. 146</u>

# Preservation of materials resulted from electronic surveillance

(1) If a decision to close a case was returned in a case, against which a complaint was not filed within the legal term set by <u>Art. 340</u> or such complaint was denied, the prosecutor shalf inform the Judge for Rights and Liberties of this forthwith.

(2) The Judge for Rights and Liberties shall order preservation of the material medium or of the certified copy of it, by archiving it at the premises of the court, in special places, in a scaled envelope, in order to ensure confidentiality.

(3) If in a case the court returned a conviction sentence, a waiver of penalty or penalty reprieve, an acquittal or a termination of criminal proceedings, which remained final, the material medium or its copy shall be preserved by being archived together with the case file at the premises of the court, in special places, by ensuring confidentiality.

#### <u>ART. 152</u>

# Obtaining data generated or processed by providers of public electronic communications networks or providers of electronic communication services intended for the public, other than the content of communications, and stored by these.

(1) Criminal investigation bodies, based on 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 data stored by it, based on the special law on storage of data generated or processed by providers of public electronic communication networks and providers of electronic communication services intended for the public, other than the content of communications, in the event that there is a reasonable suspicion related to the commission of an offense and there are grounds to believe that the

en and and an and a second

CALERA MARINA 2017 12 13

requested data represent evidence for the categories of offenses set forth by the law on the storage of data generated or processed by providers of public electronic communication networks and by providers of electronic communication services intended for the public.

(2) 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.

(3) 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.

#### <u>CHAPTER VI</u> Search and seizure of objects and documents

#### ART. 156

#### **Common provisions**

(1) Searches may be executed on: homes, persons, computers or vehicles.

(2) Searches are conducted by observing human dignity and without being a disproportionate interference in a person's private life.

#### SECTION 1 Home search

#### <u>ART. 157</u>

#### Situations and terms under which a home search may be ordered

(1) A home search or a search of goods found in a residence may be ordered if there is a reasonable suspicion that a person committed an offense or that such person is holding objects or documents that are connected to an offense and it is assumed that the search could lead to the discovery and collection of evidence related to such offense, to the preservation of traces left by the committed offense or to the capturing of the suspect or defendant.

(2) Home means a dwelling or any other space demarcated in any other way belonging to or being used by a natural person or legal entity.

#### <u>ART. 158</u>

#### Procedure for the issuance of a home search warrant

(1) Home search may be ordered during the criminal investigation, upon request by the prosecutor, by 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 of a level corresponding to it within the territorial jurisdiction of which the premises of the prosecutors' office to which the prosecutor conducting or supervising the criminal investigation belongs are located. During the trial, search is ordered by the court vested to rule in the case, ex officio or upon request by the prosecutor.

(2) An application filed by the prosecutor has to contain:

a) a description of the location where search is to be conducted, and if there is reasonable suspicion regarding the existence of a possibility of transferring searched evidence, data or persons to neighboring places, a description of such places; b) indication of evidence or data from which a reasonable suspicion related to the commission of an offense or to the holding of objects or documents linked to the offense results;

c) indication of the offense, of evidence or data from which it results that a suspect or defendant can be found or evidence related to the commission of an offense or traces of the committed offense are located at the location the search of which is requested;

d) the surname and first name and, if necessary, a description of the suspect or defendant in whose respect there are suspicions that they are at the location where the search is conducted, as well as indication of traces of a committed offense or of other objects that are assumed to exist at the venue to be subject to search.

(3) In the event that, during a search, it is found that sought evidence or data were transferred or that searched persons were hidden in neighboring places, the search warrant shall also be valid, under the law, for such places. A search continuation under these circumstances shall be approved by the prosecutor.

(4) A prosecutor shall submit an application together with the case file to the Judge for Rights and Liberties.(5) Applie discusses

(5) Applications requesting approval of a home search are ruled on within 24 hours, in chambers, without summoning the parties. The prosecutor's attendance is mandatory.

(6) The judge rules, through a court resolution, to sustain an application when this is well-grounded and approve the search, and issues a search warrant forthwith. Preparation of a hearing report is mandatory.

(7) The court resolution and the search warrant have to contain:

a) name of the court;

b) date, time and venue of issuance;

c) surname, first name and capacity of the person having issued the search warrant;

d) time frame for which the warrant was issued, which may not exceed 15 days; e) purpose for which the warrant was issued;

f) a description of the location where the search is to be conducted or, if the case may be, also of the places adjacent to it;

g) name or moniker of the person at whose domicile, residence or office the search is to be conducted, if known;

h) name of the offender, suspect or defendant, if known;

#### <u>#M2</u>

i) a description of the perpetrator, suspect or defendant who is assumed to be in the place where the search is to be conducted, indication of traces of the committed offense or of other objects that are presumed to exist at the location to be subject to search;

j) a mention that the search warrant may be used only once;

k) the judge's signature and the court's stamp.

(8) If the Judge for Rights and Liberties decides that the requirements set by <u>Art.</u> 157 are not met, they shall order, through a court resolution, dismissal of the application for conducting a home search.

(9) A court resolution through which the Judge for Rights and Liberties rules on an application for the approval of a home search is not subject to avenues of appeal.

(10) A new application for conducting a home search at the same location may be filed only if new facts or circumstances, which were not known at the moment when the previous application was ruled on by the judge, occurred or were discovered.

(11) During the trial, ex officio or upon request by the prosecutor, the court may order the conducting of a search for the purpose of enforcing a warrant for the pretrial arrest of a defendant, as well as in situations where there is a reasonable suspicion that material evidence that is connected with the offense that is the subject matter of the case exists at the location where search is requested. The stipulations of par. (2) - (8) and of <u>Art. 157</u> shall apply accordingly.

#### ART. 159

.

#### Conducting of home search

(1) A search warrant shall be communicated to the prosecutor, who shall take steps for its enforcement.

(2) Searches are conducted by a prosecutor or by criminal investigation bodies, accompanied, as applicable, by intelligence employees.

(3) A home search may not be initiated before 6:00AM or after 8:00PM, except for in-the-act offenses or when a search is to be conducted in a place open to the public at that time.

(4) If necessary, during a search, judicial bodies may restrict the freedom of circulation of present persons or the access of other persons in the place where such search is conducted.

(5) Prior to beginning a search, judicial bodies shall identify themselves and hand a copy of the warrant issued by the judge to the person whose domicile will be subject to search, to their representative or family member or, in their absence, to any other person having full mental competence who knows the person whose domicile will be subject to search and, if the case, to a trustee.

(6) In case of search conducted at the premises of a legal entity, the search warrant shall be handed to its legal representative or, in the absence of such representative, to any other person having full mental competence who is on the premises or is an employee of that legal entity.

(7) In case searches are extended to the neighboring dwellings, under the terms of <u>Art. 158</u> par. (3), persons found in such spaces shall be informed of the search extension.

(8) Prior to the initiation of a search, the persons listed under par. (5) and (6) shall be requested to hand over voluntarily the persons or objects that are sought. A search shall no longer be conducted if the persons or objects indicated in the warrant are handed over.

(9) Persons listed under par. (5) and (6) shall be informed of their right of having a counsel participate in the search conducting. If the presence of a counsel is requested, the search initiation shall be postponed until their arrival, but no longer than two hours of the moment when this right was communicated, and steps for the preservation of the venue to be subject to search shall be taken. In exceptional situations, requiring the conducting of a search on an emergency basis, or when the counsel cannot be contacted, a search can be started even prior to the expiry of the two-hour term.

(10) Also, a person subject to search shall be allowed to be assisted or represented by a trustworthy person.

(11) When a person whose domicile is searched is held in custody or arrested, they shall be brought to assist to the search. If they cannot be brought, the seizure of objects and documents and the home search shall take place in the presence of a representative or a community witness.

(12) Judicial bodies conducting a search have the right to open, by means of force, the rooms, spaces, furniture and other objects in which objects, documents or traces of an offense or persons sought could be found, in the event that their owner is not present or does not want to open them voluntarily. When opening such, the judicial bodies conducting the search have to avoid unjustified damages.

(13) Judicial bodies are under an obligation to limit only to the seizure of objects and documents that are related to the act in relation to which the criminal investigation is conducted. Objects or documents the circulation or holding of which is prohibited or in relation to which there is a suspicion that they may have connection with the commission of an offense in respect of which a criminal action is initiated ex officio shall be always seized.

(14) Exceptionally, a search may be started without handing a copy of the search warrant, without a prior request to hand over the person or objects, and without prior information the possibility to request the presence of a counsel, or of a trustworthy person, in the following cases:

a) when it is obvious that preparations are made in order to cover traces or to destroy evidence or elements that are of importance to the case ;

b) if there is a suspicion that in the space where search is to be conducted, there is a person whose life or bodily integrity is threatened;

c) if there is a suspicion that the wanted person may avoid the procedure.

(15) In the event that in the space where search is to be conducted there is no person, this shall be conducted in the presence of a community witness.

(16) In the situations listed under par. (14) and (15), a copy of the search warrant shall be handed over as soon as possible.

(17) Judicial bodies conducting a search may resort to force, in an adequate and proportional manner, in order to enter a domicile:

a) if there are well-grounded reasons to anticipate armed resistance or other types of violence or if there is a threat related to the destruction of evidence;

b) in case of a refusal or if a response was not received to any of the requests of the judicial bodies to enter the domicile.

(18) The fulfillment of process acts in the same case, which, through their nature, prevent a person whose domicile is searched to participate in its conducting shall be prohibited simultaneously with the search, except for situations where these are fulfilled, in the same case, simultaneously with other searches.

(19) The place where a search is conducted, as well as the persons or objects found during the search may be photographed or audio or video recorded.

(20) Audio-video recordings or pictures taken are to be attached to the search report and are an inherent part of it.

#### ART. 160

### Identification and storage of objects

(1) After identification, objects and documents are presented to the person from whom they are seized and to the persons in attendance, in order to be recognized and to be marked by these, so that they cannot be replaced, after which they are labeled and sealed.

(2) Objects that cannot be marked or on which labels and seals cannot be applied shall be wrapped or boxed, together if at all possible, after which seals shall be applied.

(3) Objects that cannot be seized shall be left in the custody of the person having them or of a custodian. A person to whom objects are left to keep shall be warned that they are under an obligation to keep and preserve them, and to make them available to criminal investigation bodies, upon request by these, under the sanction set forth by <u>Art. 275</u> of the Criminal Code.

(4) Evidence intended for analysis shall be taken at least in sets of two and shall be sealed. One piece of evidence shall be left with the person from which this is seized and, in their absence, to one of the persons listed under <u>Art. 159 par.</u> (11).

ART. 161 Search reports (1) Activities performed during a search are recorded in a report.

(2) Such report has to contain:

a) surname and first name and capacity of the person preparing it;

b) number and date of the search warrant;

c) venue where it is prepared;

d) dates and times when the search started and when the search ended, by mentioning any interruptions occurred;

e) surname and first name, profession and address of the persons who were present during the search, with mention of their capacity;

f) the fact that the person to be subject to search was informed of their right to contact a counsel who would participate in the search;

g) a detailed description of the places and conditions under which documents, objects of offense traces were discovered and seized, their listing and detailed description, in order to be recognized; mentions on the place or circumstances under which the suspect or defendant was captured;

h) objections and explanations by the persons who participated in the search, as well as mentions referring to the audio-video recordings or pictures taken;

i) mentions of the objects that were not seized but were left in custody;

j) mentions set forth by law for special cases.

(3) Such report shall be signed on each page and at the end by the one preparing it, by the person whose domicile was subject to search, by their counsel, if present, as well as by persons listed under par. (2) lett. e). If any of these persons is unable or refuses to sign, a mention shall be made of this, as well as of the reasons for their inability or refusal to sign.

(4) A copy of the report shall be left with the person whose domicile was subject to search or from whom objects or documents were seized or to any of the persons listed under <u>Art. 159</u> par. (5) or (6) who took part in the search.

#### <u>ART. 162</u>

#### Measures regarding seized objects or documents

(1) Seized objects or documents representing methods of proof shall be attached to the case file or kept in a different manner, and traces of a committed offense shall be seized and preserved.

(2) Seized objects, documents and traces that are not attached to the case file can be photographed. Pictures are initialed by the criminal investigation bodies and are attached to the case file.

(3) Physical evidence shall be kept by criminal investigation bodies or by the court keeping the case file until the final settlement of the case.

(4) Objects that have no connection with the case shall be returned to the person to whom they belong, except for those subject to forfeiture, under the law!

(5) Objects serving as evidence, unless subject to forfeiture, under the law, may be returned, even prior to the final settlement of the case, to the person to whom they belong, except for the situation where their restitution would impair the finding of the truth. Criminal investigation bodies or the court draws the attention of the person to whom the objects were returned that they are under an obligation to keep them until the final settlement of the case.

#### ART. 163

#### Storage or disposal of seized objects

Objects serving as evidence, if these are among those specified by Art. 252 par. (2) and are not returned, shall be stored or disposed of according the provisions of Art. 252.

#### ART. 164

# Special provisions on searches conducted at a public authority, public institution or at other public-law legal entities

A search at a public authority, public institution or other public-law legal entities shall be conducted according to the provisions of this section, as follows:

a) the judicial bodies shall identify themselves and shall hand a copy of the search warrant to the representative of such authority, institution or public-law legal entity;

b) the search shall be conducted in the presence of the representative of such authority, institution or public-law legal entity or of other persons having full legal capacity;

c) a copy of the search report shall be left with the representative of such authority, institution or public-law legal entity.

#### **SECTION 2**

#### Other forms of searches

#### ART. 165

#### Cases and situations when a bodily search is conducted

(1) Bodily search implies the examination of the exterior of a person's body, oral cavity, nose, ears, hair, clothing and of objects a person has with them or under their control at the moment of search.

(2) If there is a reasonable suspicion that, by conducting a bodily search, traces of an offense, physical evidence or other objects having importance for finding the truth in the case can be discovered, judicial bodies or any other authority having responsibilities in ensuring public order and safety shall proceed to conducting it.

#### ART. 166

.

#### Conducting of bodily searches

(1) Judicial bodies have to take steps so that a bodily search is conducted in observance of human dignity.

(2) Bodily searches are conducted by a person of the same sex as the person subject to search.

(3) Prior to beginning a bodily search, a person subject to search shall be requested to surrender the searched objects voluntarily. If the searched objects are surrendered, the search shall no longer be conducted, except for situations when its conducting is deemed useful for the search of other objects or traces.

(4) A search report has to contain:

a) surname and first name of the person subject to search;

b) surname and first name and capacity of the person having conducted the search;

c) a list of objects found on the occasion of search;

d) the place where the search is concluded;

e) date and time when the search began and date and time when the search ended, with mention of any interruptions occurred;

f) a detailed description of the place and circumstances under which the documents, objects or offense traces were discovered and seized, their listing and detailed description, in order to be recognized; mentions on the place and circumstances under which the suspect or defendant was found.

(5) Such report has to be signed on each page and at the end by the one preparing it and by the person subject to search. If the person subject to search is unable or refuses to sign, this fact shall be mentioned, along with the reasons for such inability or refusal to sign.

(6) A copy of the report shall be left with the person subject to search.

(7) <u>Art. 162</u> shall apply accordingly.

#### ART. 167

#### Vehicle search

(1) A vehicle search consists of the examination of the exterior or interior of a vehicle or of any other means of transportation or of their components.

(2) A vehicle search is conducted under the terms set by Art. 165 par. (2).

(3) Arts. 162, 165 and 166 shall apply accordingly.

#### <u>ART. 168</u>

#### Computer search

(1) 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.

(2) 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.

(3) The prosecutor shall submit an application requesting the approval of a computer search together with the case file to the Judge for Rights and Liberties.

(4) Such application is ruled on in chambers, without summoning the parties. The prosecutor's attendance is mandatory.

(5) 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.

(6) Such court resolution has to contain:

a) name of the court;

.

b) date, time and place of issuance;

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

d) the time frame for which the warrant was issued and within which the ordered activity has to be performed;

e) purpose for which it was issued;

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

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

(7) A 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.

(8) 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 stipulations of par. (1) - (7) shall apply accordingly.

(9) 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.

(10) If the seizure of objects containing computer data set under par. (1) seriously hinders the performance of activities by the persons holding such objects, the prosecutor may order the making of copies of them, which 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.

(11) A computer system or computer data storage medium search is conducted in the presence of a suspect or a defendant, and the provisions of <u>Art. 159</u> par. (10) and (11) shall apply accordingly.

(12) 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.

(13) A computer search report has to contain:

÷

a) name of the person from whom a computer system or computer data storage media is seized or name of the person whose computer system is subject to search;

b) name of the person having conducted the search;

c) names of the persons present during the search conducting;

d) a description and list of the computer systems or computer data storage media against which search was ordered;

e) a description and list of the performed activities;

f) a description and list of the computer data discovered on the occasion of the search;

g) signature or stamp of the person having conducted the search;

h) signature of the persons present during the search conducting.

(14) Criminal investigation bodies have to take steps in order 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.

(15) Computer data of a secret nature identified during such search is kept under the law.

(16) During the trial, computer search is ordered by the court, ex officio or upon request by the prosecutor, by the parties or the victim, in the situations set by par. (2). A warrant for a computer search ordered by the court shall be communicated to the prosecutor, who shall act as per par. (8) - (15).