formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

**IMPORTANT TO READ BEFORE ANSWERING THE QUESTIONNAIRE:**

The FORMOBILE project is aimed at creating better mobile forensic tools to help combat crime more efficiently, enlarging the capacities of both first responders, common forensic laboratories and highly specialised laboratories and experts by providing them with better tools to acquire, decode, and analyse data coming from mobile devices. The majority of these tools will be integrated in the existing suite of MSAB software (XRY). Please refer to the FORMOBILE website for more information and especially to the work package breakdown of WPs 4-6: https://formobile-project.eu/project#.mod-wp-steps. It is essential to have this background to be able to accurately answer this questionnaire.

One of the aspects of the FORMOBILE project is to make sure that these tools are able to be used in the EU for the collection, decoding and analysis of information from mobile phones in a way that makes the obtained evidence admissible in court ("from crime scene to courtroom").

Hence, the questions that make up this questionnaire in essence aim to understand how mobile forensic tools aimed at retrieving, decoding and further analyzing information from a mobile device (e.g. a smartphone), are allowed in your jurisdiction under the applicable criminal law. We are especially interested in:

- whether technical measures may be used (and to what extent) to bypass security;
- to what extent the data on the mobile device may be read, searched, used and copied etc.;
- what the formal conditions are for accessing data on a mobile device;
- who must order such actions and in what level of detail the mandate must describe the authorized actions;
- in what scenarios this is permissible (only in certain scenarios, only if the phone belongs to the accused?), as well as the potential differences between scenarios;
- existing limits on the access to or further analyzing and use of the data on a mobile device.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

In addition, we want to know under what conditions information on the Cloud can be accessed and if this is possible by technical means. We are also interested in any human rights' impacts, existing guidelines and issues in practice, existing case law and any other elements you deem relevant.

As we want to be able to compare answers across jurisdictions, we have drafted this request for information in a questionnaire format. This, however, does not mean we are looking for simple yes/no answers. Most questions are open questions and naturally invite an elaborate answer. Some questions may perhaps in theory be answered as yes/no question, but **please give as much guidance and details as possible within every question, to enhance our understanding of the legal system in your jurisdiction. Always cite the provision of the law or the case law you are relying on in providing an answer and please try to be exhaustive or at least as complete as possible. If you are relying on practical guidance or other informal rules and practice, please also refer to this and, if documentation on this is available, provide the link to where we can find this documentation.**

Please feel free to give additional guidance in the comments section at the end, in case you feel we did not sufficiently cover certain elements throughout the questionnaire.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

The questionnaire is made up of 61 questions, in the following sections:

- ☐ Introductory questions
- ☐ Section 1: Criminal procedure when searching/reading mobile devices, seizing mobile devices and for acquisition of data on mobile devices
- ☐ Section 2: Criminal procedure rules on analysis of data from mobile devices
- ☐ Section 3: Admissibility of evidence before court
- ☐ Section 4: Interpretation and presentation of evidence from mobile forensics before the Court
- ☐ Section 5: Implications of the use of mobiles forensics on the role of the different parties in the trial
- ☐ Section 6: Comments

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

**Introductory questions:**

***1.*** **Question:** *Please identify your organisation and your individual position?*

**Answer:** UPT – IJP – Portucalense Institute for Legal Research – Researcher

***2.*** **Question**: *Where is your organisation based?*

**Answer:** Porto, Portugal

***3.*** **Question:** *Do you have a legally defined term for a "mobile device"? If yes, what kind of devices are included within it? (e.g. Smartphones, Tablets, Smartwatches, Cameras, MP3-players, Navigation devices, Drones)*

**Answer:** No. Mobile devices such as Phones, Tablets, etc. fall under the scope of digital equipment.

**Section 1: Criminal procedure when searching/reading mobile devices, seizing mobile devices and for acquisition of data on mobile devices**

**Question***: Mobile devices (e.g. a smartphone) may enter investigations in a variety of scenarios. A suspect or a witness may have a smartphone on them during questioning or at the scene, mobile devices may be found during the search of a home or other premises, a suspect caught in the act may have a mobile device in use etc. We want to know for all these scenarios (and others you may be able to identify) what the applicable national rules are, namely answering the following questions:*

*Mobile device not seized*

***4.*** *Under what circumstances can a mobile device be read or searched without seizing it?*

The Portuguese Constitution is highly protectionist. Even when an investigation is in course a non-seized mobile device may only be searched when explicit consent is given by the person in possession of the Mobile Device.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Any evidence collected without explicit consent of the person in possession of the Mobile Device would not be admissible in Court.

This consent may be given by the person in possession of the device or by the person – natural and legal – that owns the device/ service. i.e. If a person is found in possession of a Mobile Phone/ Mobile Device that is provided by a company, the company may consent to the volunteer search.

***5.*** *Are there any limits to this search (e.g. core area of private life, privacy limits, limits defined by the crime, limits defined by the order/warrant)? If so, how precise are these/must these be defined?*

The reason behind the lack of possibility, according to Portuguese Criminal and Constitutional Laws, to look into the contents of a mobile device, are the Constitutionally foreseen right to private life, the prohibition of interference in communications and more recently, the right to anonymity and to be forgotten.

***6.*** *Is it allowed to use technical tools to bypass security?*

n/a

***7.*** *Can information be copied or only read at this stage?*

n/a

***8.*** *Is consent of the owner/person in possession of the mobile device necessary?*

Yes. In case the devise in provided by a legal person or belong to a different natural person, the later are entitled to give consent, regardless of the will of the person possessing the device.

***9.*** *Can the owner/person in possession of the mobile device be forced to unlock the device?*

No

***10.*** *Must the owner/person in possession of the mobile device be informed?*

Yes

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

***11.*** *Who can order a search and what are the formal requirements, if any?*

In general, searches require and order/ warrant by a magistrate/ Public attorney. In exceptional circunstances, the Criminal Police bodies may, in their sole motion and within their scope of action conduct stops and searches. The lawful execution of such precautionary measures as well as the admissibility of the collected evidence relays on an immediate report to the investigating judge pursuant to paragraph 6 Article 174 of the CPC, by remission on paragraph 2 of Article 251, being subject to judicial review/ confirmation.

***12.*** *Does it matter whether this person is the accused or witness/third party or the victim?*

Only the accused may have his/ her property seized.

***13.*** *What about data stored in the Cloud, what is the procedure to access/read this data if it is known or suspected to reside outside your jurisdiction? Is international cooperation like the European Investigation Order (hereinafter: EIO) or Mutual Legal Assistance Treaties (hereinafter: MLAT) the only route or do other options exist? Please elaborate.*

As mentioned above in question 4, the Portuguese Legal system does not allow the seizure and access to the contents of Mobile Devices without the consent of the owner/ person in possession of the device. Portuguese issuing authority could not use an EIO to get such data from another member State as the national legal system does not provide foresee such possibility. Such a request would be contrary to the provisions present in point b) of section 1 of Article 11 of Law nº 88/2017 that implemented the EIO Directive. Any order is limited by the scope of the corresponding applicable national proceedings. In accordance, no other process may be followed in order to obtain evidence/data, from a different legal system, in a way that would be considered inadmissible before court in accordance with the national rules on admissibility of evidence.

***14.*** *Does any of the foregoing depend on the type of crime involved (e.g. terrorism, child pornography etc.)?*

No

***15.*** *Does not following the applicable rules always lead to inadmissibility in court of the evidence in this scenario? If not, please elaborate on exceptions and relevant conditions.*

Yes

*Mobile device seized*

***16.*** *Can the mobile device (e.g. a smartphone) be seized?*

Yes

***17.*** *What are the conditions for this, who can order it and what are the formal requirements?*

Mobile devices and other objects may be seized by means of judicial an non-judicial search.

The answer will be divided in three sections. The first regards Stop and Search, as well as search (not domicile); Objects ( *"in casu"* Mobile Devices are in the possession of the searchee); Such actions do not require prior judicial order. The second regards domiciliary visits ( house search) and require prior judicial order ( Warrant). The final part of the answer concerns the seizures.

1. Article 251 of the Code of Criminal Procedure[1] ( CPC) defines Stop and Search and Search. These searches do not require prior judicial order (Search Warrant). Such measures are applicable

[1] Article 251 - **Searches** 1 - In addition to the cases provided for in Article 174 (4), criminal police bodies may proceed, without prior authorization from the judicial authority: a) Searching suspects in the event of an imminent escape or detention and searches in the place where they find themselves, except in the case of house searches, whenever they have reason to believe that objects related to crime are hidden in them, capable of serving the evidence and that otherwise they could lose up; b) Searching persons who have to participate or intend to attend any procedural act, whenever there are reasons to believe that they conceal weapons or other objects with which they may commit acts of violence. 2 - The provisions of article 174 (5) are correspondingly applicable.

according to Article 174 CPC[2]; and the formalities set forth in Art. 175 CPC[3]: exceptions exist, according to Art. 174 (5) in cases *"a) in a case of terrorism, violent or highly organised criminality, whenever there are reasonable grounds to believe that a criminal offence is to be committed, liable to jeopardize the life and the physical integrity of any person; b) if the persons concerned agree thereto, provided however that the agreement is recorded in writing; or, c) at the moment of arrest in the very act due to a criminal offence to which applies an imprisonment penalty."*[4]

Stop and search is a precautionary and police measure that may only be carried out in the cases provided for in paragraph 1 of Article 251 (a) and b)). *" in the event of an imminent escape or if the detainees have been arrested, and that it has as its premise the existence of well-founded suspicions that the suspect or the detainee hides in himself objects related to the crime and that can serve as evidence and that, otherwise, might be lost"*[5]; precautionary (or security) search is a means of preventing criminal acts to be carried out during the proceedings or in cases where the suspect is detained. Also applies when the police is sufficiently convinced that the suspect carries weapons.

The Search, also of precautionary and urgent nature (Article 251, paragraph 1, point a)), is not a home search; it applies to **the suspect** in the event of an imminent escape or on **the detainee** and requires sufficient conviction that the searched person carries objects, related to crime, that maybe present as evidence as well as the assumssion/ conviction that, had the search not been carried out the objects might be lost.

---

[2] Article 174 CPC **Assumptions** (1). The search is ordered whenever there are grounds for believing that a person is hiding any objects relating to the criminal offence or that may be useful as evidence thereof. (2). The search is ordered whenever there are any elements pointing towards the fact that the objects referred to in paragraph here above, as well as the defendant or any other person to be arrested, are in a reserved or restricted area. (3). The searches and the domiciliary visits are authorised or ordered through decision rendered by the competent judicial authority, who should preside over the act whenever possible. (4). The decision mentioned in the previous paragraph is valid for a maximum period of 30 days. After that period the decision is declared void. (5). The requirements set out in paragraph 3 do not apply to the searches and domiciliary visits performed by a criminal police department: a) in a case of terrorism, violent or highly organised criminality, whenever there are reasonable grounds to believe that a criminal offence is to be committed, liable to jeopardize the life and the physical integrity of any person; b) if the persons concerned agree thereto, provided however that the agreement is recorded in writing; or, c) at the moment of arrest in the very act due to a criminal offence to which applies an imprisonment penalty. (6). As to the cases referred to in sub-paragraph (a) of the previous paragraph the step in to be immediately communicated to the Examining Judge (Juíz de Instrução), or it will be regarded as void and nul. The Examining Magistrate must validate the step.

[3] Article 175 CPC **Formalities regarding the search** (1). Before the search takes place and except for the cases foreseen in Article 174 paragraph 5, a copy of the decision is rendered to the person concerned stating that that person is allowed to indicate a person of his/her choice to be present during the search as long as the person indicated for the effect is able to be immediately present. (2). The search must respect the personal dignity of the person and, where possible, its bashfulness.

[4] Above, footnote (1)

[5] Footnote 1 above

Article 251[6] (1) (a) of the Criminal Procedure Code is a procedural provision of an eminently precautionary nature, aimed at emergency situations in which the suspicion of the existence of evidence of a crime is not compatible with delays due to the risk of its evaporation. Its application is funded on reasonable suspission whether prior or concomitant with the intervention of the judicial authority, and according to rules of proporcionality. Paragraph b) of Article 251 is a preventive measure aimed at assuring safety and security and not the caution of evidence, it is also referred to as 'Security Search'.

The lawful execution of such precautionary measures requires immediate report to the investigating judge pursuant to paragraph 6 Article 174[7] of the CPC, by remission on paragraph 2 of Article 251, being subject to judicial review. Following GERMANO MARQUES DA SILVA[8], such validation by the investigating judge is "anomalous", considering that the Public Attorney ( PA) may require searches to be conducted. ( As a short reference for a more clear understanding of this statement: according to the Portuguese Legal System the PA is also a Judge; it acts in the interest of the people and has specific entitlements/ powers). According to PAULO PINTO DE ALBUQUERQUE[9], paragraph 2 should be subject to restrictive interpretation in the sense that the inspection of urgent investigations carried out by a criminal police body is of sole competence of the judge ( in the investigation phase) given that the remission of this legal provision exceeds the spirit of the law, "*which consists of granting the Public Attorney the competence, in the investigation phase, to order these measures* (Article 270, paragraph 2, d)[10])."

[6] Footnote 1 above
[7] Footnote 2 above
[8] Silva, Germano Marques da, Direito Processual Penal Português, Do Procedimento, Vol. 3, Lisboa, UCE, 2015
[9] Paulo Mesquita, Direcção do Inquérito e Garantia Judiciária, Coimbra, Coimbra Editora, 2003,
[10] Article 270 **Acts that can be delegated by the Public Prosecution Service to criminal police bodies** 1 - The Public Prosecution Service may entrust criminal police bodies with the responsibility of carrying out any diligences and investigations related to the investigation. 2 - Except for the provisions of the preceding paragraph, in addition to the acts that are the exclusive competence of the investigating judge, under the terms of articles 268 and 269, the following acts: a) Receive sworn statements, under the terms of the second part of paragraph 3 of article 138; b) Order the carrying out of expertise, under the terms of article 154. c) Attend an examination that may offend the person's modesty, under the second part of paragraph 3 of article 172; d) Order or authorize searches and searches, under the terms and limits of paragraphs 3 and 5 of article 174; e) Any other acts that the law expressly determines to be presided over or practiced by the Public Ministry. 3 - The Public Prosecutor's Office may, however, delegate to the criminal police authorities the power to order the execution of the expertise in relation to certain types of crime, in case of urgency or danger in the delay, namely when the expertise must be carried out jointly with the examination of traces. Except for the expertise that involves the performance of a medico-legal autopsy, as well as the provision of additional clarifications and the realization of a new expertise under the terms of article 158. 4 - Without prejudice to the provisions of paragraph 2, no. 3 of article 58, in paragraph 3 of article 243 and in paragraph 1 of article 248, the delegation referred to in paragraph 1 may be made by order of a generic nature that indicate the types of crime or the limits of the penalties applicable to crimes under investigation.

2. Article 177 of the CPC[11] defines House searches as "visits" to inhabited houses or closed dependencies. Such "visits" require prior judicial order ( search warrant) and shall be conducted between 7 am and 9 pm. Exeptions are foreseen in paragraph 2.[12]

House Searches are regulated in Article 176 of the CPC[13]; can only be carried out between 7 am and 9 pm and must be authorised by a Magistrate. A copy of the search order ( warrant) is rendered to the person who has rights over the property were the search is to take place stating its right to be present during the search as well as to be accompanied or replaced by a person of his/her choice as long the person indicated for the effect is able to be immediately present. The order may be exceptionally handed to a neighour or relative may the owner of the searched premises not be found. During the investigation stage, searches of premises other than dwellings, law offices, doctors' offices and official health establishments may be authorised or ordered by the Public Prosecutor. In specific cases a search can be carried out immediately by the Criminal Police Department, also between 9 pm and 7 am:

a) If there is good reason to believe that a crime is about to be committed in which someone's life or safety are in danger, and in cases of terrorism or violent or highly organised crime;
b) Upon consent to be searched;
c) In cases where the crime carries a prison sentence of more than three years and the individual is caught in the act.

[11] Article 177 **House search/ Domiciliary Visit** (1). Searches in an inhabited houses or in a closed dependency can only be ordered or authorized by the judge and carried out between 7 am and 9 pm, under penalty of nullity. ( 2). Between 9 pm and 7 am, home searches can only be performed in cases of: a) Terrorism or especially violent or highly organized crime; b) Consent of the target, documented in any way; c) Flagrant offense for committing a crime punishable by a maximum prison sentence of up to 3 years. (3). House searches can also be ordered by the Public Ministry or carried out by a criminal police body: a) In the cases referred to in paragraph 5 of Article 174, between 7 am and 9 pm; b) In the cases referred to in paragraphs b) and c) of the previous number, between 9 pm and 7 am. (4). The provisions of paragraph 6 of Article 174 are cor respondingly applicable in cases where the home search is carried out by a criminal police body without the consent of the person concerned and outside the act of committing an offense.(5). In the case of a search in a lawyer's office or in a doctor's office, it is, under penalty of n ullity, personally chaired by the judge, who in advance warns the president of the local council of the Bar Association or the Order of Doctors, so that the same, or a delegate, may be present. (6) In the case of a search in an official health establishment, the notice referred to in the preceding para graph and made to the president of the establishment's board of directors or management or whoever is legally substituted for it.

[12] See footnote above point (2)

[13] Article 176 **Formalities regarding the house searches/ domiciliary visits** (1). Before the domiciliary visit takes place and except for the cases foreseen in Article 174 paragraph 5, a copy of the decision is rendered to the person who has rights over the property were the s earch is to take place stating that that person is allowed to be present during the search as well as to be accompanied or replaced by a person of his/her choice as long the person indicated for the effect is able to be immediately present. (2). If the persons referred to in the previous paragraph do not appear, the copy will be delivered, whenever possible, to a relative, a neighbour, a doorman or any person replacing him/her. (3). Together with the domiciliary visit or in the course thereof any person present at the place subject to the domiciliary visit can also be searched if the person who orders or performs the search has reasonable grounds for believing that the presuppositions set out in Article 174, paragraph 1, have been fulfilled. Provisions set out in Article 173 can also be complied with.

3. Chapter III of the CPC, in Articles 178 to 186 regulates the seizure of *"objects that were meant to serve for the commission of an offence or that constitute the proceeds, profit, price or reward of it"*. Article 178 (2) provides that, whenever possible, seized objects are to be attached to the proceedings. If possible, in order to avoid its conveyance, transfer or disposition, objects are entrusted to a court official linked with the proceeding or to a custodian ( money is addressed differently but we will not address that aspects as it is not relevant for the matter).

Article 178[14] provides for the possibility of police bodies conducting a criminal investigation seizing objects used - or meant to be used - for commiting an offence, as well as those that may constitute the proceeds, profit, price or reward (also Article 249[15]).

The law does not require prior notice to allow the initial seizure property subject to confiscation. The Code of Criminal Procedure and special legislation only require rules of active legitimacy as far as the intervention of the competent judicial authority is concerned.

Article 249[16] (2) c) of the Code of Criminal Procedure provides for interim measures of protection that may be necessary to keep or preserve seized objects, so as to prevent the offender from getting rid of the assets or property derived from the commission of an offence.

***18.*** If seized, can the mobile device always be searched, information copied etc?

Yes. Digital evidence is highly volatile, sometimes just a simple push button or program execution to make it vannish. Some types of computer data are stored for short periods of time, and in other

[14] Article 178 **Objects liable to and requirements for seizure** (1). Any objects that were used or were destined for being used for the commission of a crime, as well as any objects that constitutes the proceeds of a crime, or the profit, or the price, or the recompense thereof, as well as any objects left by the perpetrator in the place where the crime was committed, as well as any other objects that could be used as evidence, shall be seized. (2). The objects seized should be attached to the proceedings, where possible; otherwise, they shall be entrusted for guardianship either to a court official linked with the proceeding, or to a custodian; all decisions should be mentioned in the referred proceeding. (3). Seizure shall be authorised, ordered or validated by way of a decision taken by the judicial authority. (4). Under the terms provided in Article 249 (2) (c), any criminal police body may seize objects in the course of body searches or the search of premises, or in circumstances of urgency, or where there is danger in delaying matters. (5). Seizures undertaken by the any criminal police body shall be submitted to validation by the judicial authority within a period of no more than 72 hours. (6). Any person who holds a title over any goods or rights seized may request to the Investigation Judge to modify the terms of, or revoke the seizure. The provisions of Article 68 (5) above, shall apply correspondingly. (7). Where the property rights over the objects seized are liable of being confiscated for the State and where such objects do not belong to the defendant, the judicial authority shall issue an order for the defendant to appear before that authority in order to hear him/her. The judicial authority shall do without the presence of the defendant when that presence is not possible.

[15] Article 249 **Protective acts as to means of evidence** (1). The criminal police bodies must perform, even before receiving order from the competent judicial authority to proceed with the investigations, the necessary and urgent protective acts to assure the means of evidence. (2). Pursuant to the previous number, it is up to them, namely: a) To proceed with examinations of the tracks of the crime, in particular to the actions foreseen Article 171 (2) and in Article 173, assuring maintenance of the state of the things and of the places; (…)

[16] idem

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

situations if the evidence is not retained quickly, this may result in significant harm to people and property[17].

The Cybercrime Law (CL)[18] establishes special Criminal Procedure rules that potentially apply to all cybercrimes, however there is no chapter devoted exclusively to the precautionary and police measures, as does the Criminal Procedure Code. Situations ought to be casuistically assessed taking both diplomas into consideration. We highlight the existence of the following – special - measures:

1. Expeditous Preservation of data, Article 12, paragraph 2[19]: The expeditious preservation of data essentially aims to prevent the loss, destruction or modification of computer data, and not to obtain computer data in itself, imposing the obligation of those who have access and control of that data to preserve it for a certain period of time. Such a process is also called "quick freeze", forcing suppliers to "freeze" the data upon notification. It does not mean that operators make data inaccessible, but access will only be done according to the specifications that were established in the court order/ Warrant. The Criminal Police Body (herein after CPB), on its own initiative, may order the preservation of data, including traffic data, when there is urgency or danger in the delay. This precautionary measure apllies to any entity, namely a service provider, with access or control of specific computer data stored in a computer system. The preservation order/ Warrant shall discriminate, under penalty of nullity, the nature of the data, its origin and destination, as well as the period of preservation. Upon being notified of this

[17] For more information on Preservation of Evidence: Bessa Vilela, Noémia & Ribeiro Henriques, Marco. (2015). Prevention from destruction of relevant evidence in cross-border cases.

[18] Lei do Cybercrime, Lei n.º 109/2009, de 15 de Setembro , available online in Portuguese language at: http://www.pgdlisboa.pt/leis/lei_mostra_articulado.php?nid=1137&tabela=leis

[19] Article 12 **Expedited preservation of data** 1 - Where, in the course of proceedings, the collection of evidence, necessary to uncover the truth, requires that specified computer data, including traffic data, that has been stored by means of a computer system, are obtained, in particular where there are grounds to believe that the computer data are particularly vulnerable to loss, modification or unavailability, the competent judicial authority shall order whoever holds or controls such data, namely the service provider, to preserve the data under consideration. **2 - Preservation may also be ordered by criminal police bodies, authorized by the competent judicial authority, or where there is urgency or danger in delay; in this last situation, the former must promptly warn the judicial authority, submitting the report provided for in article 253 of the Procedural Criminal Code**. 3 - Under pain of being deemed null and void, the preservation order must indicate: a) The nature of data; b) Their origin and destination, if known; and c) The period of time over which data must be preserved, up to three months. 4 - In compliance with the preservation order, whoever holds or controls such data, namely the service provider, shall promptly preserve the data under consideration, protecting and maintaining its integrity for the established period of time, to enable the competent judicial authority to obtain it, being subject to ensure that the undertaking of such procedures is kept confidential. 5 - The competent judicial authority may order the renewal of the measure for periods subject to the limit provided for in paragraph 3 c), insofar as the respective conditions of admissibility are met, up to a maximum limit of one year.

obligation, the supplier must preserve the data, ensuring the confidentiality of the application of the measure (Article 12 (4)[20]). The CPB should not have access to the data, limiting itself, only and exclusively, to ordering whoever has the availability of these data to preserve it. This order will be subject to be subsequent consideration, requiring validation by the competent judicial authority. The data may be preserved for a maximum period of three ( 3) months, extendable for periods not exceeding three ( 3) months, provided that the admissibility requirements are verified, up to a maximum limit of one ( 1) year, by order of the judicial authority ( Article 12[21], no. paragraphs 3 (c) and 5 of the CL). The CPB that orders the preservation of data must immediately report to the judicial authority of the fact, in accordance with the provisions of Article 253 of the Code of Criminal Procedure[22].

2. Expeditious disclosure of traffic data, Article 13[23]: This procedural measure arises in the course of a data preservation order issued by the CPB. It is intended to ensure effectiveness. It consists of the obligation of the service provider to reffer to the CPB all other suppliers through which a certain communication, whose preservation has been ordered, has been carried out, allowing the issuance of an order to preserve data for these other suppliers. ( *It should not be confused with disclosure of traffic data.).* Such information is essential in the reconstruction of the *computer path* of a given communication that is of interest for a future/ ongoing criminal proceeding, and which aims to determine its origin/destination. It is dependent on the information provided by

[20] 4 - In compliance with the preservation order, whoever holds or controls such data, namely the service provider, shall promptly preserve the data under consideration, protecting and maintaining its integrity for the established period of time, to enable the competent judicial authority to obtain it, being subject to ensure that the undertaking of such procedures is kept confidential

[21] 3 - Under pain of being deemed null and void, the preservation order must indicate: a) The nature of data; b) Their origin and destination, if known; and c) The period of time over which data must be preserved, up to three months.

[22] Article 253 - **Report** 1 - The criminal police bodies that carry out the procedures referred to in the previous articles prepare a report in which they briefly mention the investigations carried out, the results of these investigations, the description of the facts found and the evidence collected. 2 - The report is referred to the prosecutor or the investigating judge, as appropriate.

[23] Article 13 **Expedited preservation of traffic data** In order to ensure the preservation of traffic data related to a specific communication, regardless of whether one or more service providers were involved in the transmission of that communication, the service provider which was ordered to perform such preservation pursuant to the preceding article shall indicate to the judicial authority or to criminal police bodies, as soon as this information is available to it, other service providers through which the communication was made, in order to identify the service providers and the path through which the communication was transmitted.

each of the service providers through which the communication passed, and obtaining such information quickly and in time is essential for the success of the investigation.

3. Seizure of computer data, Article 16[24], paragraph 2: The CPB may seize, on its own initiative, when there is an urgency or danger of not securing or losing evidence if there is sound conviction that certain data or computer documents serve or have served the practice of criminal offenses - Article 16. no. 2[25] of the CL. The legitimacy of such seizures builds upon communication to and validation by the judicial authority, within 72 hours ( Article 16, no. 4[26] of the CL ). The lack of the aforementioned step results on inadmissibility of the collected evidence. The law does not ignore that personal computers are the place where personal/ confidential documents are kept, photographs, films or sound recordings that are likely to reveal secrets and that are manifestations of their owner's private or intimate life. (Article 16, no. 3[27] of the CL foresees the penalty for nullity of all evidence that violates the rights of the owner of the equipment as well as of third parties. Such regime aims at safeguarding the right privacy and intimacy of the owner of data or computer documents, or of a third party, values constitutionally enshrined in Article 35 of the Constitution of the Portuguese Republic[28]. Such elements

[24] Article 16 **Seizure of computer data** 1 - Where, in the course of a computer system search, or of another legitimate means of access to a computer system, computer data or documents necessary to the collection of evidence, in order to uncover the truth, are found, the competent judicial authority shall authorize or order the seizure thereof. 2 - Criminal police bodies are entitled to perform seizures, without any prior authorization from the judicial authority, in the course a computer system search lawfully ordered and executed pursuant to the preceding article, or where there is urgency or danger in delay. 3 - In case of seizure of computer data or documents the contents of which may disclose personal or intimate data, thus hindering the privacy of the respective holder or of a third party, on pain of being deemed null and void such data or documents shall be submitted to the judge, who shall weight their attachment to the file, taking into account the interests of the case. 4 - Seizures carried out by criminal police bodies shall always be validated by the judicial authority, within at the most 72 hours. 5 - Seizures related to computer systems used for legal, medical and bank practises shall comply with the rules and formalities provided for in the Criminal Procedure Code, duly adapted, and those related to computer systems used by journalists shall comply with the rules and formalities provided for in the Journalists Statute, duly adapted. 6 - The regime governing professional, staff and State secret information, provided for in article 182 of the Criminal Procedure Code, shall apply, duly adapted. 7 - Seizure of computer data, depending on what is deemed to be most appropriate or proportional, taking into account the interests of the case, may take the following forms: a) Seizing the computer system support equipment or the computer-data storage medium, as well as devices required to read data; b) Making a copy of those computer data, in an autonomous means of support, which shall be attached to the file; c) Maintaining by technological means the integrity of data, without copying or removing them; or d) Removing the computer data or blocking access thereto. 8 - In the situation of seizure provided for in point b) of the preceding paragraph, copies shall be made in duplicate, one of them being sealed and entrusted to the court clerk of services where the case has been brought and, where technically possible, seized data shall be certified by means of a digital signature.

[25] idem

[26] idem

[27] idem

[28] Article 35 (**Use of information technology**) 1. Every citizen has the right of access to all computerised data thatconcern him, which he may require to be corrected and updated, and the right to be informed of the purpose for which they are intended, as laid down by law. 2. The law shall define the concept of personal data, together with the terms and conditions applicable to its automatised treatment and its linkage, transmission and

must be brought before the judge in a closed envelope, the latter being the first to know of its content, thus avoiding the exposure of the holder or third parties to other agents. Article 16 paragraph 7 [29]of the CL establishes the need to comply with the principles of proportionality and adequacy of seizure in view of the interests of the specific case. It also defines the different ways of capturing computer data, which may be: the "support on which the system is installed or (...) computer data are stored, as well as the devices necessary for the respective reading" (paragraph a)); make a "copy of the data, in autonomous support", (paragraph b)); preserving the integrity of the data, "by technological means (...) without making copies or removing them" (paragraph c)); or eliminate itself in a non-reversible way or block access to data (paragraph d)). The legislator has imposed that the seized data must be certified through a digital signature, which is a measure of preservation and guarantee of the integrity of the seized data preventing any alteration in the collected evidence - Article 16, paragraph 8[30], of the CL. This Article also requires that if the seizure is carried out by copying the data in an autonomous way, it must be done in duplicate. DIAS RAMOS proposes to ammend the used word in the diploma "copy" with expressions such as "*cloning*" or "*image copy*", as these are forensic computer equipment and tools for this purpose, which through the creation of a digital summary (hash code) allows to certify that the evidence has not been tampered with.

4. Preservation and prompt disclosure of computer data on international cooperation, Article 22, paragraph 4.[31]: The effectiveness of the collection of digital evidence is

use, and shall guarantee its protection, particularly by means of an independent administrative entity. 3. Information technology may not be used to treat data concerning philosophical or political convictions, party or trade union affiliations, religious faith, private life or ethnic origins, save with the express consent of the datasubject, or with an authorisation provided for by law and with guarantees of non- discrimination, or for the purpose of processing statistical data that are not individually identifiable. 4. Third-party access to personal data is prohibited, save in exceptional cases provided for by law. 5. The allocation of a single national number to any citizen is prohibited. 6. Everyone is guaranteed free access to public-use information technology networks. The law shall define the regime governing cross-border data flows, and the appropriate means for protecting both personal data and other data whose safeguarding is justified in the national interest. 7. Personal data contained in manual files enjoy the same protection as that provided for in the previous paragraphs, as laid down by law.

[29] Above, footnote 24

[30] idem

[31] Article 22 **Expedited preservation and disclosure of computer data in international cooperation** 1 - Portugal may be requested to obtain the expeditious preservation of data stored by means of a computer system, located within Portuguese territory, for criminal offences provided for in

directly related to the speed of the intervention, and such objectives can only be achieved through the use of mutual assistance in terms of precautionary measures and police cooperation, which allow to face the challenges posed by the crime developed in the "Computing Era". This measure aims at the preservation of stored computer data, carried out according to Article 12 paragraph 2[32] of the CL, in a computer system located in Portugal; preventing data from being altered, removed or deleted during the period of time necessary for the preparation, transmission, and execution of a request for mutual assistance for the purpose of obtaining the data. This is a precautionary measure at the reach of the CPB when there is urgency or danger in the delay, as an answer to a request by a foreign judicial authority, with a view to the future submission of a request for legal aid for the purposes of research, seizure and disclosure of computer data. This request from a foreign judicial authority is submitted via "contact point 24.7", which provides immediate assistance.

***19.*** *Are there any limits to this search (e.g. core area of private life, privacy limits, limits defined by the crime, limits defined by the order/warrant)? If so, how precise are these/must these be defined?*

article 11, and in respect of which the requesting Party intends to submit a request for mutual assistance for the search, seizure or disclosure of the data. 2 - A request for preservation shall specify: a) The authority seeking the preservation; b) The offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts; c) The computer data to be preserved and its relationship to the offence; d) Any available information identifying the custodian of the computer data or the location of the computer system; e) The necessity of the preservation; and f) The intention to submit a request for mutual assistance for the search, seizure or disclosure of data. 3 - In order to execute the request from the competent foreign authority pursuant to the preceding paragraphs, the competent judicial authority shall order whoever holds or controls such data, namely the service provider, to preserve them. 4 - The preservation may also be ordered by the Polícia Judiciária, by means of an authorization from the competent judicial authority or where there is urgency or danger in delay, and in this case the provision in paragraph 4 of the preceding article shall apply. 5 - Under pain of being deemed null and void, the preservation order must indicate: a) The nature of data; b) Their origin and destination, if known; and c) The period of time over which data must be preserved, up to three months. 6 - In compliance with the preservation order, whoever holds or controls such data, namely the service provider, shall promptly preserve the data under consideration for the specified period of time, protecting and maintaining their integrity. 7 - The competent judicial authority, or the Polícia Judiciária by mean of an authorization from the former, may order the renewal of the measure for periods subject to the limit provided for in paragraph 5 c), insofar as the respective conditions of admissibility are met, up to a maximum limit of one year. 8 - Upon receiving the request for assistance referred to in paragraph 1, the judicial authority with powers to decide on the matter shall determine the preservation of data until a final decision is taken on the request. 9 - Data preserved under this article shall only be provided: a) To the competent judicial authority, to execute the request for assistance referred to in paragraph 1, as if a similar national situation were at stake, pursuant to articles 13 to 17; b) To the national authority that issued the preservation order, as if a similar national situation were at stake, pursuant to article 13. 10 - The national authority which receives, pursuant to the preceding paragraph, a communication on traffic data to identify the service provider and the path through which the communication was transmitted, shall communicate them promptly to the requesting authority, to enable that authority to submit a new request for expedite preservation of computer data. 11 - Paragraphs 1 and 2 hereof apply, duly adapted, to requests made by Portuguese authorities.

[32] Above, Footnote 19

The limits to searcher are clearly defined. Limitations to evidence acquired by means search apply, as mentioned above, in accordance with Article 35 of the Constitution of the Portuguese Republic[33] and with Article 34[34] of the same diploma, when regarding emails/ sms and other evidence that falls under the scope of correspondence/ home.

***20.*** *Is consent of the owner/person in possession of the mobile device ever a relevant element?*

No.

***21.*** *Can the owner/person in possession of the mobile device (if identified) be forced to unlock the device?*

No. "Nemo tenetur se detegere" "Nemo tenetur se ipsum accusare" "Nemo tenetur se ipsum prodere"; the action of unlocking a Mobile Device cannot be imposed. One of the fundamental and constitutional principles of Portuguese criminal law is the privilege against self-incrimination, which applies both to criminal and administrative procedures. is means that the defendant is under no obligation to assist investigations, or to provide any elements that may lead to self-incrimination (i.e., the defendant may remain silent with minimal intervention, awaiting the nal decision).

[33] Article 35 (**Use of information technology**) 1. Every citizen has the right of access to all computerised data thatconcern him, which he may require to be corrected and updated, and the right to be informed of the purpose for which they are intended, as laid down by law. 2. The law shall define the concept of personal data, together with the terms and conditions applicable to its automatised treatment and its linkage, transmission and use, and shall guarantee its protection, particularly by means of an independent administrative entity. 3. Information technology may not be used to treat data concerning philosophical or political convictions, party or trade union affiliations, religious faith, private life or ethnic origins, save with the express consent of the datasubject, or with an authorisation provided for by law and with guarantees of non- discrimination, or for the purpose of processing statistical data that are not individually identifiable. 4. Third-party access to personal data is prohibited, save in exceptional cases provided for by law. 5. The allocation of a single national number to any citizen is prohibited. 6. Everyone is guaranteed free access to public-use information technology networks. The law shall define the regime governing cross-border data flows, and the appropriate means for protecting both personal data and other data whose safeguarding is justified in the national interest. 7. Personal data contained in manual files enjoy the same protection as that provided for in the previous paragraphs, as laid down by law.

[34] Article 34 (**Inviolability of home and correspondence**) 1. Domiciles and the secrecy of correspondence and othermeans of private communication are inviolable. 2. Entry into a citizen's domicile against his will may only be ordered by the competent judicial authority and then only in the cases and in compliance with the forms laid down by law. 3. No one may enter any person's domicile at night without his consent, save in situations of flagrante delicto, or with judicial authorisation in cases of especially violent or highly organised crime including terrorism and trafficking in persons, arms or narcotics, as laid down by law. 4. The public authorities are prohibited from interfering in any way with correspondence, telecommunications or other means of communication, save in the cases in which the law so provides in matters related to criminal procedure.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

***22.*** *Must the owner/person in possession of the mobile device be informed? If so, about what exactly?*

Yes.

***23.*** *Is it allowed to use technical tools to bypass security measures and/or anti-forensic measures?*

Yes.

***24.*** *Does it matter whether this person is the accused or witness/third party or the victim?*

Only the accused/ supect of having committed a crime may have the Mobile Devices seized.

***25.*** *What about data stored in the Cloud, what is the procedure to access this data if it is known or suspected to reside outside your jurisdiction? Is international cooperation like the European Investigation Order or Mutual Legal Assistance Treaties the only route or do other options exist? Please elaborate.*

The only route to obtaining the information saved in a cloud outside of the umbrella of the Portuguese law lays in international cooperation, in all its forms.

***26.*** *What about data stored in the Cloud, where you are unable to determine the location of the server or the identity of the service provider?*

As before.

***27.*** *Can you legally access data in the Cloud, even if there is no app that links to this data or other direct link from the mobile device?*

Yes, as long as the information is hosted in a Portuguese server. Such access must be orders by a judge.

The search for computer data corresponds *"roughly"* to a search for data in a digital environment, which is why the search execution regime provided for in the Criminal Procedure Code applies (see Article 15[35], paragraph 6) of Cybercrime Law).

However, in the event that it is necessary for the proof, with a view to discovering the truth, to obtain specific and determined computer data, stored in a certain computer system, the competent judicial authority (which consists of the Public Prosecutor in charge of an investigation) authorizes or orders that a search be made in that same computer system. It can never be stressed enough that there is a provision that allows only the search for stored computer data, thus not allowing the interception of communications in progress.

Furthermore, if in the course of such research reasons arise to believe that the data sought are found in another computer system (or in a different part of the same computer system), paragraph 5 of Article 15[36] of the Cybercrime Law, by means of authorization/ order of the competent authority, the possibility of extending the search to such a system as long as the data are legitimately accessible from the initial system, which is of increasing practical importance today, taking into account, for example, social networks, servers of email or clouds.

***28.*** *How is the access to data kept by a Service Provider related to the device regulated? Is it performed upon a Court order, or also through other means?*

As above.

[35] Article 15 **Search of computer data** 1 - Where, in the course of proceedings, the collection of evidence, necessary to uncover the truth, requires that specified computer data, stored in a specific computer system, are obtained, the competent judicial authority shall authorize or order the search to that computer system, overseeing such investigations whenever possible. 2 - The order provided for in the preceding paragraph shall be valid for a maximum period of 30 days, on pain of being deemed null and void. 3 - Criminal police bodies shall undertake the search, without a prior authorization from the judicial authority: a) Where whoever holds or controls data under consideration voluntarily consents to the search, insofar as the consent is documented in any way; b) In cases of terrorism, violent or highly-organized crimes, or where there is evidence to substantiate the imminent commission of a criminal offence threatening the life or integrity of any person. 4 - Where criminal police bodies undertake the search pursuant to the preceding paragraph: a) In the situation provided for in point b), the investigation shall be promptly communicated to the competent judicial authority, and assessed by the latter as far as the validation of the measure is concerned, on pain of being deemed null and void; b) In any other situation, the report provided for in article 253 of the Criminal Procedure Code shall be drawn up and submitted to the competent judicial authority. 5 - Where, in the course of the search, there are grounds to believe that the data sought is stored in another computer system or part of it, and such data is lawfully accessible from the initial system, the search may be extended to the other system, by means of an authorization or order from the competent authority, pursuant to paragraphs 1 and 2. 6 – To the search referred to herein shall apply, duly adapted, the rules on execution of searches provided for in the Criminal Procedure Code and in the Journalists Statute.

[36] idem

The issuance, by the Public Prosecutor of an order the search for computer data must be substantiated, containing the reasons why such diligence is necessary to discover the truth, and is valid for 30 days. The diligence to search for computer data must be chaired by a magistrate, and if this proves to be impossible, the aforementioned impossibility must be justified in the search order, which may be the rule taking into account the difficulties of order practice that such a requirement would place on the efficient time management of each magistrate.

On the other hand, in the situations identified in Paragraph 3 of Article 15[37] of the Cybercrime Law, the CPB may carry out search on computer data, without the need for prior authorization from the judicial authority, however, reporting to the judicial authority is mandatory, with a view to obtain validation for te searcg, as well as the preparation and referral of the report provided for in Article 253 of the Code of Criminal Procedure[38].

***29.*** *Does any of the foregoing depend on the type of crime involved (e.g. terrorism, child pornography etc.)?*

No.

***30.*** *Does not following the applicable rules always lead to inadmissibility of the evidence in this scenario? If not, please elaborate on exceptions and relevant conditions.*

Yes.

[37] idem
[38] Above, footnote 22.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

*Please, answer all these questions separately for each scenario or instance which, in your opinion, is (partially) subject to different rules than other scenarios. At least, make the difference between the scenarios where a mobile device is seized and where it is not. If all sub-scenarios in one of these scenarios are the same, it suffices to only answer the questions once. However, most jurisdictions have different situations in which seizure is possible (e.g. in the context of a search of premises vs. not in the context of a search), so please differentiate between these scenarios, as well and answer the questions for them separately. If you prefer, you can answer the questions in their totality in an integrated explanation, as long as all elements are covered and again, various scenarios are differentiated between.*

**Please, give as much guidance as possible to enhance our understanding. Always cite the provision of the law or the case law you are relying on (legal basis) and mention conditions, people involved in the action, formal requirements etc., even if not specifically asked.**

**Answer:** Indication of length of answer: at least a couple of pages, as this is the main overview question.

***31.* Question**: *In cases where the examination or data acquisition is not possible without changing the configuration of the device, is there a strict protocol that should be followed (e.g. procedure and changes should be tested, validated, and documented)? If yes, please specify on what rules this is based and what the requirements are. Please also provide examples.*

There are no legal provisions on this matter.

***32.* Question:** *Are there any specific rules in criminal procedure that regulate the use of mobile forensics tools using/deploying AI technology? Are there any conditions which need to be met so AI-powered tools could be applied in the process of evidence collection?*

No. There are not such rules in the Portuguese Legal System.

***33.* Question:** *What are the main legal issues in your jurisdiction in the cases when mobile devices are involved in crimes across geographical boundaries? What procedures are foreseen to*

*tackle these multijurisdictional issues? Should the forensic examiner be aware of the nature of the crime and the regional laws/legislative framework?*

The question does not apply to the Portuguese Legal System. The only geographic restriction exist when the crime has been commited in the territory of another country or in cases when the evidence is stored in servers outside of the Portuguese territory.

***34.* Question:** *Is there an established procedure/course of action to decide whether to apply the EIO or another instrument for cross-border gathering of evidence within the EU?*

Article 5 of Law nº 88/2017 regulates the types of proceeding where an EIO may be issued.

The law states that an EIO can be issued in criminal proceedings that are initiated by a judicial authority / by that authority according to the internal legal order of the issuing State; proceedings that can be initiated by judicial authorities relative to facts that are punishable under the law of the issuing State so long as the decisions can be appealed to a judicial body; proceedings that are initiated by administrative bodies relative to facts that are punishable under the law of the issuing State; proceedings relative to crimes or other punishable acts involving the responsibility or punishment of non-human legal persons according to the laws of the issuing State.

Questions regarding the issuing authority are regulated in Article 12 of Law nº 88/2017. According to this legal precept an EIO can be issued by the national judicial authority that has the competence to steer a specific phase of the proceedings. An EIO can also be issued by the national EUROJUST member. Finally, an EIO can also be issued by the competent administrative entity regarding the violation of administrative rules. However, it must be validated by the State Prosecution Office.

***35.* Question:** *Since, the abovementioned Directive does not preclude the application of MLAT by judicial authorities under some circumstances, what is the practice in your jurisdiction?*

**Answer:** Indication of length of answer: 1-2 paragraphs.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

***36.* Question:** *Are you aware of any existing cooperation mechanisms and practices with the private sector?*

No

**Section 2: Criminal procedure rules on analysis of data from mobile devices**

***37.* Question:** *When data has been made accessible through mobile forensics, are there any rules on how the data must be analysed, especially to take into account:*

- *Data protection concerns (Law Enforcement Directive 2016/680 and implementing national law)*
- *Privacy concerns and respect for core area of private life (i.e. how is it guaranteed that very sensitive information, not relevant to the investigation is not used)*
- *Human rights such as the right to a fair trial (tools may deliver faulty results and methods used are often untransparent) and the right to non-discrimination (tools that are untransparent may contain bias)*
- *What information can be retained/copied? For how long?*

*Please elaborate on both criminal procedure law, relevant data protection law and any other measures or guidelines that may exist. Please also cite and explain relevant case law.*

**Answer:** Indication of length of answer: couple of paragraphs.

**Section 3: Admissibility of evidence before court**

***38.* Question:** *Are there general rules or guidelines on the admissibility of electronic evidence in your jurisdiction applicable to mobile forensics, not yet discussed above?*

Despite some recently implemented legislation that has conferred digital evidence a certain regulated "autonomy" especially rules on the retention/ admission of data generated or processed in connection with the provision of electronic communications services services or of public

communications. in Law 32 / 2008, of 17 July, and with the procedural rules contained in the Cybercrime Law, the truth is that there is no particular density or normative rules in this area.

Such difficulty in the legal framework results, in large part, from the complexity of electronic evidence, indelibly associated with the very complexity of cyber "reality".

In fact, electronic evidence suffers from its own frailnesss, requiring to be treated with care, to the extent that a mere carelessness can effectively render it unusable. Moreover, precisely due to its complexity and "delicatness", DIAS RAMOS considers that, among the typified evidential classifications, electronic evidence should be included in the "expert evidence" cathegory (as it requires qualified technical knowledge from those who collect it), despite of the "immateriality" of electronic evidence (which is not susceptible to material seizure[39]), it can also be classified as documentary evidence (insofar as "it can be embodied in writing or by other technical means, such as, for example, the photographic or audiovisual impression of an email message"[40]). Thus, the criminal investigator who apprehends the digital evidence has to know how to deal with this specific type of evidence (not only in apprehension, transport and handling but also in its subsequent analysis). Such need led to the implementation of yet another legal diploma aimed at regulationg the conservation of data generated or processed in the context of the provision of electronic communications services (Law No. 32/2008, of 17 July).

Regardless of the categorization that is made of this type of evidence, the general principles that impose restrictions and limits on all means of obtaining evidence shall apply. In this context, for example, the principle of investigation (or material truth) endows the court with the power to order the gathering of all the necessary evidence to discover the material truth of the facts. Such collection of evidence is bond to the principle of procedural truth (raising questions of admissibility, so that

[39] In truth an " electronic document [texts, sounds, imagens, etc.] is nothing but a sequence of binary numbers ( 0; 1) that, processed and translated by the computer, contains information" ; presented in the form of " bits, instead of having been printed or signed in paper; its authenticity verificabillity and track of circulation ought to be conducted electronically".. (BRENO LESSA, *apud* MILITÃO, Renato Lopes, *A Propósito da Prova Digital no Processo Penal*, Faculdade de Direito e de Ciências Sociais e Humanas da Universidade de Lisboa).
[40] DIAS RAMOS, *A Prova* ..., op. cit., p. 97

there is no excess in the search for material truth). Equally important is the principle of free assessment of evidence[41].

It should also be noted that, following SILVA RODRIGUES, the specific principles contained in the International Hi-Tech Crime and Forensics Conference of October 1999 apply, in addition to the principles relating to evidence contained in Code of Criminal Procedure.

Having made a small introduction, it is important to clarify that, according to the Portuguese Legislation, ***mobile forensics*** is a search carried out in a computer system; for that reason, general rules on collection, validity and admissibility apply.

***39.*** **Question:** *Are the criteria for admissibility of evidence collected through mobile forensics the same as for the other types evidence? Please elaborate in any case.*

Regardless of the fact that the Portuguese Legislation does not provide for any specific provision on collection/ admissibility nor validity of ecidence collected by means of computer forensics, general rules apply.

***40.*** **Question:** *What if procedural rules are not followed? Can evidence from mobile forensics still be submitted to the Court in certain circumstances, balancing out the interest of the criminal justice with the severity of the procedural breach?*

In case of breach of applicable procedural rules, the collected means of evidence will not be admissible before court. According to the Portuguese law, the breach of any procedural step during the collection and storage of evidence in criminal proceedings results in thenullity of the evidence, if presented before court ( as question 18, above).

[41] Article 127 of the Code of Criminal Procedure establishes that *"unless the law provides otherwise, the evidence is assessed according to the rules of experience and the free conviction of the competent entity").*

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

***41.* Question:** *Specifically, if data in the Cloud is accessed according to criminal procedure, but it turns out to be located outside your jurisdiction does this mean it is not admissible at all? Is it relevant that there was reasonable doubt about the location of the data at the time?*

As before. The breach of any applicable rules of procedure during collection/ validation or handeling of evidence results in absolute inadmissibility of evidence. Only evidence collected in a *Cloud* hosted in a Portuguese server could be directly by the forensics team.

***42.* Question:** *What are the consequences if mobile evidence are altered either intentionally, or unintentionally due to their dynamic nature during the investigation process? Note that intentional alteration refers to using a process to uncover data which is known to alter some (meta)data, not to the falsification of evidence. The question is more whether any alteration, even on small and not relevant data may render the evidence inadmissible.*

As mention above in question 18, Article 16 paragraph 7 of the CL establishes the different ways of capturing computer data, which may be: the "support on which the system is installed or (...) computer data are stored, as well as the devices necessary for the respective reading" (paragraph a)); make a "copy of the data, in autonomous support", (paragraph b)); preserving the integrity of the data, "by technological means (...) without making copies or removing them" (paragraph c)); or eliminate itself in a non-reversible way or block access to data (paragraph d)). The legislator has imposed that the seized data must be certified through a digital signature, which is a measure of preservation and guarantee of the integrity of the seized data preventing any alteration in the collected evidence. Any – even the slightest – alteration of the collected data will result in the inadmissibility of all the collected data, hence making the evidence null, if presented before Court.

***43.* Question:** *Specifically, are there rules on the used technology, methodology or standard, such as for example that this must be forensically sound as a prerequisite for admissibility? If yes, please elaborate.*

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

No such rules exist.

***44.* Question:** *Are you aware of existing case-law in your jurisdiction, dealing with the admissibility of evidence produced using mobile forensics? If yes, please elaborate.*

**Answer:** Indication of length of answer: 1-2 paragraphs.

***45.* Question:** *Is there in your jurisdiction an established and recognised standardisation(s) of the processes of collection, analysis, interpretation and reporting of digital evidence that must be followed for the evidence to be admissible? (as critical to the validity of evidence, their quality and impact evidence's acceptance by the courts)? If yes, please elaborate.*

Portugal has a general data retention system that is regulated by Law nº 32/2008, 17th July, that implemented Directive 2996/24/EC relative to the conservation of data generated or treated in the context of electronic communication services that are publicly available or from public communication networks. Both Directive and law that transposed it create an obligation for providers to conserve/retain certain data for the purpose of investigation, detection and repression of certain serious crimes by the authorities. The data can accessed upon request by the CPB and the Pubic Prossecutor and is dependent of a judicial decision. Data is conserved or retained for a period of one year. Furthermore, the law foresees the approval of a regulation - approved by Regulation 469/2009 - that establishes the terms as well as the technical and security conditions for the electronic communication and transmission of data relating to traffic and localization information relative to persons or legal entities as well as the data necessary to identify the subscription holder or registered user.

As mentioned above the regular chain of evidence applies to digital evidence as well as to mobile forensics.

The Portugueselaw does not differenciate between digital and non digital collection/ validation process.

***46.* Question:** *Is a failure to comply with Data Protection law, or privacy rules in itself, enough to refuse admissibility of the evidence, even when procedure is otherwise followed?*

Yes, as above. Any violation of Constitutionally foreseen principles/ rules shall result in total loss of the collected evidence as it will be deemed inadmissible.

***47.* Question:** *Is there case law in your jurisdiction on evidence collected through mobile forensics having been questioned or rejected in Court because the admissibility was questioned? If yes, please elaborate on at least 3 cases.*

**Yes.**

**Section 4: Interpretation and presentation of evidence from mobile forensics before the Court**

***48.* Question:** *Are there general rules or guidelines on the interpretation and presentation of evidence from mobile forensics, such as:*

- *Is mobile forensic evidence given a certain probative value?*
- *Are there rules on how to interpret mobile forensic evidence or requirements which must be complied with for the evidence to be considered reliable?*
- *Must such evidence be examined by an expert witness?*
- *If not obligatory, is this a common practice?*
- *What are the requirements for experts (experience, independence, training, etc.)?*
- *Is there a centralised management of mobile forensic operations in your jurisdiction to ensure the work is compliant with standards and can be presented in court in a consistent manner?*

There are no rules on the probative value to be applicable to the evidence gathered by means of mobile forensics. Mobile forensics, itself, it not sufficiently defined in the Potuguese diplomas related to cybercrime/ collection of evidence in matters not related to cybercrime.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

Analogy would lead the rapporteur to give evidence obtaind by means of mobile forensics of the strength of expert opinion. At the same time, the doctrime is split as some authors, such as COSTA ANDRADE, stand by the conviction that evidence collected/ gathered by means of mobile forensics ( such as images, emails, and other documents) should be analysed in the light of the same rules applicable to documental evidence and not expert reports/ opinions. At the same time, the report that follows with the collected evidence is written by an expert officer, specializes in computer/ digital forensics.

Ideally, a centralized system ought to be in place, ensuring maximum compliance and consistency in both collection and appreciation of evidence by the judge. The Portuguese Legal System does not foresee the existebce of such a centralized management system. All gathered evidence is assessed by the presiding judge according to his/her understanding/ conviction/ assessment.

***49.* Question:** *Are you aware of existing case-law in your jurisdiction dealing with the interpretation and presentation of evidence produced using mobile forensics? If yes, please elaborate.*

**Answer:** Indication of length of answer: 1-2 paragraphs.

***50.* Question:** *Is there in your jurisdiction an established and recognised standardisation(s) of the processes of collection, analysis, interpretation and reporting of digital evidence that must be followed for the interpretation and presentation of evidence before a court? Or alternatively which is not obligatory but considered as critical for the validity of evidence, its quality or the impact of the evidence and its acceptance by the courts? If yes, please elaborate.*

The following procedures do not hinder the validity of the evidence. They aim solely at harmonizing the overall process of collecting evidence and reporting to the court.

Request of data from Data Operators:

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

In view of the need to articulate and harmonize procedures for requests for data from telecommunications operators, the Public Prossecutor Office developed a cooperation protocol to apply while investigating cybercrime and obtaining digital evidence.

In fact, the aforementioned operators are of significant importance in the context of the preservation, storage and production of information necessary to produce evidence in criminal proceedings. In this sense, Circular No. 12/2012, of September 25, 2012, of the Public Prossecutor Office, enshrined a set of uniform forms of procedures, more defining a range of guidelines in order to facilitate the satisfaction of communications operators of requests for collaboration of the Public Ministry.

Thus, the Public Prosecutor's Office has a set of pre-prepared forms available in the Public Prosecutor's Information System, both regarding requests for data preservation in criminal proceedings and requests for information. In the former, the Public Ministry, using the means of obtaining evidence (or precautionary measures) provided for in Articles 12 and 13 of the Cybercrime Law, indicates the nature of the data to be preserved, the period covered, as well as, if possible, the origin and destination of the data, and may also request, as soon as other service providers are known through which communications have been made, information in order to identify all service providers used by those communications. As for requests for information, it is permitted, under the terms of Article 14 of the Cybercrime Law, to obtain various types of computer data: IMEI numbers, mobile phone numbers, identification of phone holders with their personal data, holders e-mail accounts, IP address used to access the e-mail account, all available elements for identifying the user of a given IP in a given time context, among many others.

It is, however, important that the request from the Public Prosecutor's Office is proportional to the need of the investigation , as well as that in each request the respective objective is specified, which translates, above all, in the concrete indication of the data that is intended to obtain/ retain .

Furthermore, in addition to requests for data from telecommunications operators, the Public Prossecutor has other essential tools available in the field of collecting and obtaining digital evidence, without the need to resort to international cooperation mechanisms, namely forms to be addressed to the Facebook, Instagram, YouTube, Microsoft, Google, among other foreign entities,

which are simple and expeditious to use by any public prosecutor, even if they do not have relevant computer knowledge, and which thus allow, for example, obtaining data regarding the identification of the account holder (name, address and IP address from which the account was opened).

Finally, it is also necessary to reaffirm that it is the Public Prosecutor's Office, within the scope of its powers to conduct investigations, that is responsible for requesting information from service providers, and should not delegate this task to a criminal police body.

Data consisting of Personal Data or correspondence

Articles 16, 3, and 17, of the Cybercrime Law are not absolutely clarifying as regards the timing and form of intervention by the investigating judge in the case of seizure of personal or intimate data and email or records of communication with a similar nature.

Indeed, as far as the first of the aforementioned precepts is concerned, it has already been mentioned above that the entity competent to order the seizure of computer data is the Public Ministry; however, if data or documents revealing personal or intimate data that may jeopardize the privacy of the respective holders are apprehended, it is necessary to present the data to the investigating judge who will consider joining them to the case file taking into account the interests of the case. concrete. Thus, the literal content of the Article seems to point in the sense that the legitimate intervention of the Public Ministry is enough for the criminal police organ to seize the data, and the investigating judge only intervenes if personal or intimate data is seized.

Now, in view of the above, the question that arises in practice is whether it is due to the Public Ministry, without having a precise notion of what can be found in the course of a search (home or not), followed by seizure of support, research and seizure computer data, to request, a priori, before carrying out the aforementioned steps, to the investigating judge, to join the records of what may be found. On the one hand, such a procedure could remedy the legislative definition of what are personal or intimate data, not leaving in the hands of the criminal police body the concretization of such a concept.

On the other hand, this does not seem to have been the intention of the legislator. Thus, when the Public Prosecutor issues search warrants (or promotes home searches), it can immediately also order the search and seizure of computer data, informing the criminal police body of the procedure that must be adopted in the case provided for in Article 16 (3) of the Cybercrime Law. In the event of the seizure of intimate or personal data, which could jeopardize the privacy of the respective holders, the records must be presented, in an autonomous support, to the Public Prosecutor, who will present them to the investigating judge, justifying the reasons why, taking into account the interests of the specific case, such data must be attached to the file.

Corresponde and other communication data

The case of Article 17 of the Cybercrime Law contains substantially divergent outlines.

In fact, in relation to electronic mail or records of a similar nature, it is the judge who determines the apprehension of those who prove to be of great interest for the discovery of the truth or for the evidence. In this sense, the question that arises here is related to the prior requirement of a judicial order to order the seizure of the aforementioned messages. That is to say, the Public Prosecutor's Office, pending the investigation, should encourage judicial intervention in order to authorize the seizure of messages that may be found in the course of a computer search or other legitimate access to a computer system before such actions are carried out. evidentiary steps?

The law is not absolutely clear, so it is possible to adopt two perspectives. One in the sense that the court order ordering the seizure must be prior. In other words, the Public Prosecutor's Office may order computer research, data seizure (with the specificity of Article 16, paragraph 3, of the Cybercrime Law, regarding personal or intimate data), but it would have to be the judge of instruction to pre-order the seizure of electronic mail or similar messages. In this light, if prior judicial authorization was obtained, the hypothesis that such data would be found in the course of legitimate access to a computer system would be safeguarded, despite the fact that the investigating judge was not effectively aware of them, which could result in too much dispatch being made generic, almost providing a true blank letter to the investigation, it is not possible to weigh the values that the precept in question requires.

The other position, which seems to us to be the most correct procedure for the procedural management of the investigation by the Public Prosecutor, is the precautionary / provisional seizure of electronic mail or similar messages by such judicial authority, with the judicial order being only later. Thus, the Public Prosecutor's Office may authorize the computerized search of data (or other legitimate form of access to the computer system), and if messages are found, they are provisionally apprehended (or, perhaps, informally), and must subsequently , the Public Prosecutor presents such messages, in an autonomous support, to the investigating judge, who will determine, depending on whether they are of great interest in discovering the truth or in the evidence, their definitive (or formal) seizure and consequent addition to the case file.

In this sense, it has to be understood, contrary to what happens with the correspondence seizure regime, that the investigating judge is not the first person to know the content of the apprehended correspondence, which may be the criminal police body or the Public Ministry . In fact, it can only be so because computer research itself (or other legitimate access to the computer system) can immediately compel the investigative entity to be aware of the content of the messages, which, therefore, immediately filter the messages with relevance to the specific case, only referring them to the investigating judge.

Other investigation steps

There is a wealth of other investigative steps that a more proactive prosecutor in the direction of the investigation can do on its own, without the need for delegation to other entities, and that do not require specific technical knowledge.

From the outset, of course, any search can be made in the different search engines available on the Internet, such as Google, Bing, Yahoo, Sapo, which can take on important shapes in certain contexts.

It is also possible to obtain information regarding the practice of criminal offenses on social networks. It is well known that their proliferation has created new types of crime and developed new ways to practice existing criminal offenses. Many of the pages, profiles, online groups, through which such crimes are committed, are public, thus being accessible by anyone, enabling the collection and obtaining of digital evidence by the Public Prosecutor.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

***51.* Question:** *Is there case law in your jurisdiction on evidence collected through mobile forensics having been questioned or rejected in Court because of interpretation issues or presentation issues (e.g. considered admissible but not reliable)? If yes, please elaborate on at least 3 cases.*

**Answer:** Indication of length of answer: 3+ paragraphs.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

## Section 5: Implications of the use of mobiles forensics on the role of the different parties in the trial

**52. Question:** *Are there rules or guidance, or is there case law in your jurisdiction on how to respect the right to a fair trial in case of evidence extracted via mobile forensics? What practices are established in view of the respect of the principle of equality of arms?*

Nuch such rules exist in the Portuguese Legal System. The right to a fair trial is ensured by the Constitutional Law of the Portuguese Republic in Articles 20[42] and 32[43] and Articles 57 to 67 of the Code of Criminal Procedure[44].

[42] Article 20 **(Access to law and effective judicial protection)** 1. Everyone is guaranteed access to the law and the courts in order to defend those of his rights and interests that are protected by law, and justice may not be denied to anyone due to lack of sufficient financial means. 2. Subject to the terms of the law, everyone has the right to legal information and advice, to legal counsel and to be accompanied by a lawyer before any authority. 3. The law shall define and ensure adequate protection of the secrecy of legal proceedings. 4. Everyone has the right to secure a decision in any suit in which he is intervening, within a reasonable time limit and by means of fair process. 5. For the purpose of defending the personal rights, freedoms and guarantees and in such a way as to secure effective and timely judicial protection against threats thereto or breaches thereof, the law shall ensure citizens judicial proceedings that are characterised by their swiftness and by the attachment of priority to them.

[43] Article 32 **(Safeguards in criminal proceedings)** 1. Criminal proceedings shall ensure all necessary safeguards for the defence, including the right to appeal. 2. Every defendant shall be presumed innocent until his sentence has transited in rem judicatam, and shall be brought to trial as quickly as is compatible with the safeguards of the defence. 3. Defendants shall possess the right to choose counsel and to be assisted by him in relation to every procedural act. The law shall specify those cases and phases of proceedings in which the assistance of a lawyer shall be mandatory. 4. Preliminary investigations shall be conducted entirely under the responsibility of a judge, who may, subject to the terms of the law, delegate the practise of such investigative acts as do not directly concern fundamental rights to other persons or bodies. 5. Criminal proceedings shall posses an accusatorial structure, and trial hearings and such preliminary investigative acts as the law may require shall be subject to the principle of pleading and counter-pleading. 6. The law shall define the cases in which, subject to the safeguarding of the rights of the defence, the presence of the defendant or the accused at procedural acts, including trial hearings, may be dispensed with. 7. Victims shall possess the right to take part in proceedings, as laid down by law. 8. All evidence obtained by torture, coercion, infringement of personal physical or moral integrity, improper intromission into personal life, the home, correspondence or telecommunications shall be deemed null and void. 9. No case shall be withdrawn from a court that already had jurisdiction under an earlier law. 10. Defendants in proceedings concerning administrative offences or in any proceedings in which penalties may be imposed shall possess the right to be heard and to a defence.

[44] Article 57 **The status of defendant (arguido)** 1 – Any person formally charged or against whom the beginning of the examining stage (instrução) has been requested in the scope of criminal proceedings shall acquire the status of defendant. 2 – The defendant's status shall remain valid during all stages of proceedings. 3 – The provisions of Article 58, paragraphs 2 to 6, shall apply accordingly.
Article 58 **Acquiring the status of defendant** 1 – Subject to the provisions of Article 57, the formal acquisition of the status of defendant is mandatory as soon as: a) A person makes statements before any judicial authority or criminal police body during an inquiry started against him, where there are grounds to suspect that such person has committed a criminal offence; b) A coercive or patrimonial guarantee measure must be imposed on a specific person; c) A suspect is arrested under the terms and for the purposes of Articles 254 to 261 of this Code; or d) A police report has been drawn up identifying a person as an alleged offender and such person has been informed on the contents thereof, unless the report is clearly ungrounded. 2 – The status of defendant is acquired by the communication to the concerned person, either orally or in writing, by a judicial authority or criminal police body that, as of that moment, he has the status of defendant in criminal proceedings and, if necessary, by the explanation of procedural rights and duties of defendants laid down in Article 61, which he, therefore, is bound to observe. 3 – The status of defendant following communication by a criminal police body is reported to the judicial authority within 10 days. The judicial authority shall have a 10-day period for examination and validation or non-validation of the act. 4 – The status of defendant implies the handing over to the concerned person, if possible simultaneously, of a document specifying the particulars of the case and those of his defence counsel, should the latter have been appointed. The document must also indicate the defendant's procedural rights and duties as listed in Article 61. 5 – Failure to comply with, or breach of, the formalities laid down in the preceding paragraphs shall prevent the use as evidence of any statements made by the concerned person. 6 – The non-validation of the status of defendant by the judicial authority does not affect evidence previously collected.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

***53.* Question:** *Is there any training required by law for the judges, prosecution, expert witnesses, lawyers involved in cases with evidence coming from mobile forensics?*

---

Article 59 **Other cases entailing the acquisition of the status of defendant** 1 – Should, in the course of an interview to a person other than a defendant, grounded suspicions that such a person committed a criminal offence be raised, the authority conducting such interview shall immediately suspend it and proceed to the communication and to the advice referred to in Article 58(2). 2 – The person suspected of having committed a criminal offence has the right to be acquire the status of defendant, at his/her own request, whenever investigations conducted for purposes of confirming such suspicions personally affect him/her. 3 – The provisions of Article 58(3)(4) shall apply accordingly.
Article 60 **Procedural status** From the moment when a person acquires the status of defendant, he is ensured the exercise of procedural rights and duties, without prejudice to the enforcement of coercive and patrimonial guarantee measures or to the implementation of evidence formalities, as provided for by law.
Article 61 **Procedural rights and duties** 1 – Unless otherwise provided for by law, a defendant has, at all stages of proceedings, the right to: a) Attend all procedural acts that directly affect him; b) Be heard by the court or by the examining judge whenever they render a decision that personally affects him; c) Be informed on charges against him prior to making any statements before an authority; d) Refuse answering any questions addressed by an authority on charges against him and on the substance of his statements on them; e) Choose a lawyer or ask the court to appoint him a defence counsel; f) Be assisted by a defence counsel in all procedural acts where he takes part and, when detained, to contact such counsel in privacy; g) Take part in the inquiry and examination, propose evidence and require any necessary measures; h) Be informed on his rights by the judicial authority or criminal police body before which he must appear; i) Appeal, under the law, against any decisions to his detriment. 2 – Communication in privacy as referred to in subparagraph f) above shall occur in a visible manner whenever required for security reasons, but may not be overheard by the watching agent. 3 – A defendant has especially the duty to: a) Appear before the judge, prosecutor or criminal police body whenever required by law and after being summoned; b) Answer truthfully to questions addressed by the competent authority on his identity; c) Fill in the form Termo de Identidade e Residência (Statement of Identity and Residence) as soon as he acquires the status of defendant; d) Submit to evidence formalities and to coercive and patrimonial guarantee measures, as specified by law and as ordered and implemented by a competent authority.
Article 62 **Defence counsel** 1 – Defendants may choose a lawyer at any stage of proceedings. 2 – If a defendant has more than one chosen lawyer, service of process will be made in relation to the lawyer having been chosen in the first place during the formal declaration as defendant.
Article 63 **Rights of defence counsels** 1 – The defence counsel exercises the rights recognised by law to defendants, except for those personally granted to the accused. 2 – A defendant may render without effect any acts performed on his behalf by the defence counsel, as long as he does it by an explicit statement before a decision on that act is taken.
Article 64 **Compulsory assistance** 1 – The assistance by a defence counsel is compulsory: a) During the interrogation of an arrested or detained defendant; b) During interrogation by a judicial authority; c) During the preliminary hearing and court hearings; d) In any procedural acts other than the formal declaration as defendant, whenever the accused person has any visual, hearing or speaking impairment or is illiterate, can not speak or understand the Portuguese language, is less than 21 years old, or where the issue of his excluded or diminished criminal liability has been raised; e) In case of ordinary or extraordinary appeal; f) In cases provided for by Articles 271 and 294; g) Where the trial hearings take place in absence of the defendant; h) In other cases determined by law. 2 – Besides cases referred to above, the court may appoint a defence counsel for a defendant, at the court's or defendant's request, where the specific circumstances of the case show the need or the convenience for the defendant to be assisted. 3 – Subject to the provisions of paragraphs above, if the defendant does not have a lawyer or an appointed defence counsel, the appointment of a counsel is compulsory as of the moment when the person is formally charged. The identification of the defence counsel shall be mentioned on the court order that closes the inquiry. 4 – In the case provided for by paragraph 3 above, the defendant shall be informed, on the charge document, that, if he is found guilty, he must pay the defence counsel's fees except if he granted legal aid, and that he may replace the defence counsel by a lawyer of his choice.
Article 65 **Assistance to several defendants** Where there is more than one defendant in the same case, they may be assisted by a single defence counsel, if that does not hamper the actions of the said defence counsel.
Article 66 **Appointed counsel** 1 – The appointment of a defence counsel is notified to the defendant and to the defence counsel when they are not present in the act. 2 – The appointed counsel may be exempted from the case if he invokes a reason that the court finds fair. 3 – The court may always replace the appointed counsel at the defendant's request, on reasonable grounds. 4 – Until he is replaced, the counsel appointed for an act shall perform his duties in subsequent acts of the case. 5 – The appointed counsel performs his duties against , whose amount and terms shall bedecided by the court, within limits set forth at the tariff adopted by the Ministry of Justice, or considering fees normally paid for similar services. The payment shall be made, accordingly, by the defendant, the party assisting the public prosecutor (assistente), the civil parties or the Justice Ministry Treasury.
Article 67 **Replacement of a defence counsel** 1 – If, regarding an act implying the need for assistance, the defence counsel does not appear, if he leaves before the act is finished, or refuses to exercise or quits defence, the court shall immediately appoint another defence counsel. However, if an immediate appointment is not possible or adequate, the court may also decide to interrupt the act. 2 – If the defence counsel is replaced during the examining debate or hearing, the court may, ex officio or upon request of the new defence counsel, provide for an interruption, so that the new defence counsel may discuss the case with the defendant and examine the files. 3 – Instead of the interruption mentioned above, the court may choose, if absolutely necessary, to postpone the act or the hearing for not more than five days.

No specific training is required. Special training sessions are conducted to judges on a volunteer basis at CEJ ( Centro de Estudos Judiciários). No other law related profession can access for free legal training in such matter. Special teams regarding computer/ mobile forensics do exist and are an integrated part of the Portuguese Criminal Investigation Police. Such experts are from the field of IT/ Cumputer sciences/ Networks/ Engineering.

***54.* Question:** *Is there a pre-determined time duration/limitation period required for the extraction of evidence from mobile devices, time for decoding, reviewing and analysing of the data, time for reporting that data in a form that prosecutors and others can use?*

As mentioned above in question 18, The data may be preserved for a maximum period of three ( 3) months, extendable for periods not exceeding three ( 3) months, provided that the admissibility requirements are verified, up to a maximum limit of one ( 1) year, by order of the judicial authority ( Article 12, no. paragraphs 3 (c) and 5 of the Cybercrime Law).

***55.* Question**: *What are the procedural rights inherent to the different participants in a criminal procedure (i.e. the prosecution, the court, the defendant, the witness, the victim, etc.)?*

Defendant/ Defender:

Pre-trial:

a) Before questioning a person against whom there is enough suspicion and an investigation is being carried out against, this suspect has to be held as a defendant, as established in Article 58[45]

[45] Article 58 **Acquiring the status of defendant** 1 – Subject to the provisions of Article 57, the formal acquisition of the status of defendant is mandatory as soon as: a) A person makes statements before any judicial authority or criminal police body during an inquiry started against him, where there are grounds to suspect that such person has committed a criminal offence; b) A coercive or patrimonial guarantee measure must be imposed on a specific person; c) A suspect is arrested under the terms and for the purposes of Articles 254 to 261 of this Code; or d) A police report has been drawn up identifying a person as an alleged offender and such person has been informed on the contents thereof, unless the report is clearly ungrounded. 2 – The status of defendant is acquired by the communication to the concerned person, either orally or in writing, by a judicial authority or criminal police body that, as of that moment, he has the status of defendant in criminal proceedings and, if necessary, by the explanation of procedural rights and duties of defendants laid down in Article 61, which he, therefore, is bound to observe. 3 – The status of defendant following communication by a criminal police body is reported to the judicial authority within 10 days. The judicial authority shall have a 10- day period for examination and validation or non-validation of the act. 4 – The status of defendant implies the handing over to the concerned person, if possible simultaneously, of a document specifying the particulars of the case and those of his defence counsel, should the latter have been appointed. The document must also indicate the defendant's procedural rights and duties as listed in Article 61. 5 – Failure to comply with, or breach of, the

(1) a) of the CPC. The rights and duties of a defendant are set in Article 61[46] of the CPC, and these are of mandatory information to the suspect, then defendant, in that same act. These rights are: right to be present at any procedural act that directly affects them; to be heard by the court or examining magistrate every time a decision that personally affects them is made; to be informed of the facts they are suspected of having commited before giving a statement to any authority; right to remain silent; right to be assisted by a lawyer or request that one is appointed; right to be assisted by a legal counsel in every procedural act they have to participate in and, whenever arrested, to contact with their lawyer in private; to participate in the investigation and the instruction stages by providing evidence and requesting needed measures; to be informed by the criminal police authority or judicial authority to which they must give a statement of the rights they have; to appeal of any decision against them. They shall also be informed of the procedure to follow to request that a legal counsel is nominated in case of financial hardship, as established in Law 34/04, of the 29th of April. Every defendant is put into statement of identity and residence (coercive measure) after the act of holding as a defendant, in a continuous act.

The act of holding someone as a defendant when made by the criminal police authority needs to be communicated to the competent judicial authority (which can either be the public prosecutor or the examining magistrate, depending on the case), in order to be evaluated and validated. Communication by the police to the judicial authority has to be made within 10 days and the confirmation by the judicial authority also needs to be provided within 10 days, as established in Article 58 (3)[47] of the Criminal Procedure Code.

---

formalities laid down in the preceding paragraphs shall prevent the use as evidence of any statements made by the concerned person. 6 – The non-validation of the status of defendant by the judicial authority does not affect evidence previously collected.

[46] Article 61 **Procedural rights and duties** 1 – Unless otherwise provided for by law, a defendant has, at all stages of proceedings, the right to: a) Attend all procedural acts that directly affect him; b) Be heard by the court or by the examining judge whenever they render a decision that personally affects him; c) Be informed on charges against him prior to making any statements before an authority; d) Refuse answering any questions addressed by an authority on charges against him and on the substance of his statements on them; e) Choose a lawyer or ask the court to appoint him a defence counsel; f) Be assisted by a defence counsel in all procedural acts where he takes part and, when detained, to contact such counsel in privacy; g) Take part in the inquiry and examination, propose evidence and require any necessary measures; h) Be informed on his rights by the judicial authority or criminal police body before which he must appear; i) Appeal, under the law, against any decisions to his detriment. ´´ 2 – Communication in privacy as referred to in subparagraph f) above shall occur in a visible manner whenever required for security reasons, but may not be overheard by the watching agent. 3 – A defendant has especially the duty to: a) Appear before the judge, prosecutor or criminal police body whenever required by law and after being summoned; b) Answer truthfully to questions addressed by the competent authority on his identity; c) Fill in the form Termo de Identidade e Residência (Statement of Identity and Residence) as soon as he acquires the status of defendant; d) Submit to evidence formalities and to coercive and patrimonial guarantee measures, as specified by law and as ordered and implemented by a competent authority.

[47] Above footnote 45

If the defendant is under arrest (in order to be put into custody the suspect needs to be held as a defendant), the defendant has further rights of which he or she shall be informed, adding up to the mandatory information about the rights and duties established in Article 61[48].

When arrested, the suspect, shall be informed of the reasons for the arrest in the moment of the arrest. This information should include the facts and corresponding legal basis (Article 27[49] (4) of the Portuguese Constitution and Article 258[50] (1) c) of the CPC). The rights and duties of the defendant, however, are communicated in the later moment of holding someone as a defendant. Before questioning, the defendant will also be informed of why he or she will be questioned. In case of detained defendant, he or she shall always be heard by a judicial authority (examining magistrate and before that by a public prosecutor if it is not possible to proceed with first judicial questioning immediately), within 48 hours, that shall confirm the arrest or free the defendant.

During police questionings, the defendant shall furthermore be informed (aside from, once more, the rights established in Article 61) of the reasons for the arrest (Article 141 (4) c)[51]); and the exact

[48] Above footnote 46

[49] Article 27 **Right to freedom and security** 1. Everyone has the right to freedom and security. 2. No one may be wholly or partially deprived of their freedom, except as a consequence of a judicial conviction and sentence imposed for the practice of an act that is legally punishable by a prison term or the judicial imposition of a security measure. 3. The following cases of deprivation of freedom for the period and under the conditions laid down by law are exceptions to this principle: a) Detention in flagrante delicto; b) Detention or remand in custody due to strong indications of the wilful commission of a crime that is punishable by imprisonment for a maximum term of more than three years; c) The imprisonment or detention of, or the imposition of any other coercive measure subject to judicial control on, a person who improperly entered or improperly remains in Portuguese territory, or who is currently the object of extradition or deportation proceedings; d) The disciplinary imprisonment of military personnel, which imprisonment is subject to the guarantee of appeal to the competent court; e) The subjection of a minor to measures intended to protect, assist or educate him in a suitable establishment, when ordered by the competent court of law; f) Detention by judicial decision for disobeying a court decision or to ensure appearance before a competent judicial authority; g) Detention of suspects for identification purposes, in the cases that are and for the time that is strictly necessary; h) Committal of a person suffering from a psychic anomaly to an appropriate therapeutic establishment, when ordered or confirmed by a competent judicial authority. 4. Every person who is deprived of his freedom must immediately be informed in an understandable manner of the reasons for his arrest, imprisonment or detention and of his rights. 5. Deprivation of freedom contrary to the provisions of the Constitution or the law places the state under a duty to compensate the aggrieved person in accordance with the law.

[50] Article 258 - **Arrest warrants** 1 - Arrest warrants are issued in triplicate and contain, under penalty of nullity: a) The signature of the competent judicial authority or criminal police; b) The identification of the person to be detained; and c) Indication of the fact that motivated the arrest and the circumstances that legally justify it. 2 - In case of urgency and danger in the delay, it is permissible to request detention by any means of telecommunication, followed immediately by warrant confirmation, under the terms of the previous number. 3 - The arrest warrant is presented to the detainee and delivered one of the copies. In the case of the previous number, the arrest warrant containing the requisition, the indication of the judicial authority or criminal police that made it and the other requirements referred to in paragraph 1, and a copy thereof, are displayed.

[51] Article 141 **First preliminary court examination of an arrested defendant** 1 – The arrested defendant who is not to face trial immediately shall be examined by the Examining Judge within forty-eight hours following his/her arrest and for such a purpose a detailed description of the grounds for the arrest and of the evidence supporting such an arrest is given. 2 – The examination is exclusively conducted by the Examining Judge, with the assistance of a Public Prosecutor and of the defense counsel and in the presence of a court clerk. The presence of any other person shall not be allowed unless, for security reasons, the person arrested must be kept in sight by the police. 3 – Questions regarding his/her name, parents, place of birth, date of birth, civil status, profession, home address and workplace shall be put to the defendant who may be required, if necessary, to show a valid official identification document. He/she shall be warned about the fact that he/she shall be held criminally liable should he/she fail to answer these questions or provide false answers. 4 – The Examining Judge shall then inform the defendant of the following: a) The rights referred to in article 61(1), explaining such rights to him/her if necessary; b) Should he/she choose not to remain silent, the statements made by him/her might be

facts he or she is suspected of having committed, including, whenever known, the time, place and feature of the circumstances (Article 141 (4) d)). This information shall be included in the report of the police questioning (Article 141 (4) in fine).

When a defendant is arrested, information about the reasons for the arrest needs to be provided. When a person is arrested outside of a flagrante delicto an arrest warrant is needed (Article 257 (1) of the CPC). Therefore, the facts that led to the arrest and the circumstances that form the legal basis for the arrest are written in the arrest warrant, a copy of which will be delivered to the defendant (Article 258[52] (3) of the CPC). In case of urgency and danger caused by delay, however, detention can be ordered by any means of telecommunications and confirmed in writing immediately afterwards (Article 258[53] (2) of the CPC).

Finally, the information provided during an interrogation is given orally. However, this information is written as part of the report of the interrogation, all information except the rights established in Article 61[54] and read in the beginning of the questioning are there registered (Article 141[55] (4) of the CPC in fine), but it is stated that the defendant was informed of them. Even though to the present date only the first judicial hearing of a defendant (Article 141[56] (7) of the CPC) and the

used in the court of law, even if he/she is tried in absentia or makes no statements during the trial hearing, and shall be subject to a free assessment of the evidence; c) Of the reasons behind his/her arrest; d) Of the acts of which he/she stands accused, including, if known, the circumstances of time, place and method; and e) Of the elements contained in the case file and that evidence the charges brought, whenever the communication of such elements does not jeopardize the investigation, does not hamper the discovery of the truth and does not endanger the life, the physical or psychological integrity or the freedom of the parties to the case or of the victims of the crime; and all the information, except the one foreseen in sub-paragraph a) above, shall be included in the records made for questioning purposes. 5 – When making statements, the defendant may confess or deny the facts and his/her participation in them and point out the causes that may exclude the unlawfulness or guilt, as well as any circumstances that may be relevant for determining his/her responsibility or for setting the specific extent of the sentence. 6 – During the examination, the Public Prosecutor and the defense counsel shall, without prejudice to the right of invoking nullities, refrain from any interference. The judge may allow them to make requests for the clarification of the answers given by the defendant. Once the examination is concluded, they may ask the judge to put questions to the defendant deemed relevant for the discovery of the truth. The judge shall decide, by means of an order from which no appeal shall lie, whether the request shall be made in the presence of the defendant and whether the questions to be put are relevant. 7 – The defendant's examination is carried out, as a general rule, through sound or audiovisual recording. Other means may only be used, namely stenographic or stenotype means or any other technical mean capable of ensuring the full reproduction of the questions put and the answers given, or the documentation through court records, when the means preferred are not available. The said information shall then have to be included in the records. 8 – Whenever the questions put and the answers given are the object of sound or audiovisual recording, the time when the recording started and ended must be included in the records. 9 – The provisions laid down in article 101 shall apply accordingly.

[52] Above Footnote 50
[53] Idem
[54] Footnote 46
[55] Above footnote 51
[56] idem

court hearing (Article 364 (1)[57] of the CPC) are also registered through recording (audio or audiovisual), this possibility can be used as well in other hearings and questionings, including police questioning, as established in Article 141 (7) of the CPC.

During court hearings

a) The defendant is personally informed of the day the court hearing will take place through a written notice that includes: naming the facts the defendant is accused of and respective legal provisions (it may be made by referral to the accusation); the place, date and time of the hearing; appointing the legal counsel if the defendant still does not have one; and it is dated and signed by the judge (Article 313[58] (1) a) to d) of the CPC). This is a personal notice to the defendant (Article 113 (10)[59]). and it shall be served together with a copy of the accusation.

[57] Article 364 - **Form of the documentation** 1 - The documentation of the statements made orally at the hearing is carried out, as a rule, through an audio or audiovisual record, only other means, namely shorthand or shorthand, or any other technical means suitable for use, may be used. ensure full reproduction of those, when those means are not available. 2 - In addition to the statements made orally at the hearing, the information, clarifications, requirements and promotions are subject to the audio or audiovisual record, as well as the respective responses, orders and oral allegations. 3 - When there is an audio or audiovisual record, the beginning and the end of each of the acts listed in the previous number must be recorded in the minutes. 4 - The secretariat transcribes requests and the respective responses, orders and decisions that the judge, unofficially or upon request, determines by unappealable order. 5 - The transcription is made within five days, counting from the respective act; the deadline for arguing any non-conformity in the transcript is five days, counting from the notification of its incorporation in the records. 6 - The provisions of article 101 are correspondingly applicable.

[58] Article 313 **Court order setting the date for the main hearing** 1 – The order setting the date for the main hearing must contain, under penalty of nullity: a) An account of the facts and relevant legal provisions, which can be done by referring to the indictment or charge document, if any; b) An indication of the venue, day and time for the hearing; c) The appointment of a counsel for the defendant, if a lawyer has not yet been chosen for the proceedings; and d) The date and signature of the presiding judge. 2 – The court order, together with a copy of the charge or indictment document, is notified to the public prosecutor, as well as to the defendant and his defence counsel, to the party assisting the public prosecutor (assistente), to the civil parties and their representatives, at least 30 days prior to the date set for the main hearing. 3 – Service of process on the defendant and on the party assisting the public prosecutor (assistente) under the preceding paragraph takes place as provided for by Article 113, paragraph 1, subparagraphs a) and b), except where they have indicated their address or workplace to the police or judicial authority that draws up the information report or hears them during the inquiry or examination stage and where they have never reported a new address by registered letter; in this case, service of process shall take place by simple postal delivery, under Article 113, paragraph 1, subparagraph c). 4 – The court order appointing the date for the main hearing cannot be appealed against.

[59] Article 113 - General rules on notifications 1 - Notifications are made through: a) Personal contact with the notifier and in the place where he is found; b) Registered post, by registered letter or notice; c) Simple postal delivery, by letter or notice, in the cases expressly provided for; or d) Public notices and announcements, in cases where the law expressly allows it. 2 - When made by registered post, notifications are presumed to have been made on the third day following that of their sending, when it is useful, or on the first business day following that, when it is not, and the applicable fee must be included in the act of notification. 3 - When made by simple postal means, the judicial official draws a quota in the file indicating the date of dispatch of the letter and the address to which it was sent and the postal service distributor deposits the letter in the notifying's mailbox, draw up a statement indicating the date and confirming the exact location of the deposit, and send it immediately to the sending service or court, considering the notification made on the 5th day after the date indicated in the statement drawn up by the postal service distributor , which must be included in the notification act. 4 - If it is impossible to deposit the letter in the mailbox, the postal service distributor draws up a note of the incident, sets the date and immediately sends it to the sending service or court. 5 - Subject to the provisions of paragraphs 3 and 4, notifications by simple post referred to in paragraph d) of paragraph 4 of article 277, which are sent without proof of deposit, and the employee must draw up a quota in the process indicating the date of dispatch and considering the notification made on the 5th business day after the date of dispatch. 6 - When the notification is made by registered post, the face of the envelope or notice must indicate, precisely, the nature of the correspondence, the identification of the sending court or service and the rules of procedure referred to in the following paragraph. 7 - If: a) The recipient refuses to sign, the postal service agent delivers the letter or notice and draws up a note of the incident, the act being valid as a notification; b) The addressee refuses to receive the letter or the notice, the postal service agent draws up a note of the incident, the act being valid as a notification; c) The addressee is

During trial the defendant is informed by the judge of the defendant's right to make a statement at any moment during the court hearing and to the defendant's right to remain silent, as established in Article 343 (1)[60] of the CPC.

Absence of the defendant from the court hearing is only allowed in very exceptional occasions, therefore the rule is that presence in court is an obligation (as well as a right) of the defendant. However, the defendant can go away from the court room if he or she was already questioned and the court does not deem his or her presence absolutely necessary, being therefore represented by his or her legal counsel (Article 332[61] (5) of the CPC). The same applies for situations in which the

not found, the letter or the notice is delivered to the person who lives with him or the person indicated by the addressee who works with him, the postal services mentioning the fact with identification of the person who received the letter or the notice ; d) It is not possible, due to the absence of a person or for any other reason, to proceed under the terms of the previous paragraphs, the postal services comply with the provisions of the respective regulations, but whenever they leave notice they will expressly indicate the nature of the correspondence and the identification of the court or the sending service. 8 - Notices and communications made are valid as notification, except in cases where the law requires different form: a) By judicial or criminal police authority to the interested parties present in a procedural act presided over by it, as long as documented in the record; b) By telephone in case of urgency, if the requirements contained in paragraph 2 of the previous article are respected and if, in addition, in the telephone call you are notified that the summons or communication is valid as a notification and the telephone call is followed by confirmation telegraph, telex or fax. 9 - The notifying party may indicate a person, with a residence or professional domicile located in the area of territorial jurisdiction of the court, for the purpose of receiving notifications. In this case, the notifications, carried out in compliance with the formalism provided for in the previous paragraphs, are considered to have been made to the person notifying himself. **10 - Notifications of the accused, the assistant and the civil parties can be made to the respective defender or lawyer. Noteworthy are the notifications regarding the prosecution, the instructing decision, the designation of the day for trial and the sentence, as well as those relating to the application of coercion and equity guarantee measures and the deduction of the claim for civil compensation, which, however, must also be notified to the appointed lawyer or defender; in this case, the period for the practice of a subsequent procedural act starts from the date of the last notification.** 11 - Notifications to the appointed lawyer or defender, when not otherwise provided by law, are made electronically, under the terms to be defined in an ordinance of the Government member responsible for the area of justice, or, when this is not possible, in terms of paragraphs a), b) and c) of no. 1, or by fax. 12 - When made electronically, notifications are presumed to be made on the third day after their dispatch, when it is useful, or on the first business day following that, when it is not. 13 - The public notice is made by posting a public notice on the door of the last residence of the notifying party and another in the places for that purpose designated by the respective parish council, followed by the publication of an advertisement in the area of digital services of the courts, accessible at the address https://tribunais.org.pt. 14 - In the cases expressly provided for, with several defendants or assistants, when the period for the practice of acts subsequent to the notification ends on different days, the act can be practiced by all or by each one of them until the end of the period that began to run. last. 15 - The signature of the official responsible for drafting the notification can be replaced by an indication of the identification code of the notification, as well as the address of the Ministry of Justice website where, by inserting the code, it is possible to confirm the authenticity of the notification.

[60] Article 343 - **Defendant's statements** 1 - The President shall inform the defendant that he is entitled to make statements at any time during the hearing, provided that they refer to the subject of the process, without however being obliged to do so and without the your silence may disadvantage you. 2 - If the accused is willing to make statements, the court will hear him in all he says, within the limits indicated in the previous paragraph, without expressing any opinion or making any comments from which a judgment on guilt can be inferred. 3 - If, in the course of declarations, the defendant turns away from the object of the process, reporting the matter that is irrelevant to the good decision of the case, the president warns him and, if the latter persists, withdraws the floor. 4 - Responding to several co-defendants, the president determines whether they should be heard in the presence of each other; in the event of a separate hearing, the President, once all the defendants have been heard and returned to the hearing, briefly gives them knowledge, under penalty of nullity, of what has happened in their absence. 5 - The Public Prosecutor's Office, the defender and representatives of the assistant and civil parties are not allowed to interfere with the defendant's statements, namely suggestions as to how to declare. However, with respect to the defender, the provision in the second part of paragraph 1 of article 345.

[61] Article 332 - **Presence of the defendant** 1 - The presence of the defendant at the hearing is mandatory, without prejudice to the provisions of paragraphs 1 and 2 of article 333 and in paragraphs 1 and 2 of article 334. 2 - The accused who must answer before a certain court, according to the general rules of jurisdiction, and is imprisoned in a different district for the practice of another crime, is requested to the entity that has him at his order. 3 - At the reasoned request of the defendant, it is up to the court to provide him with the conditions for his displacement. 4 - The defendant who has attended the hearing cannot leave the hearing until the end. The President takes the necessary and appropriate measures to avoid removal, including detention during interruptions to the hearing, if that seems essential. 5 - If, despite the provisions of the preceding paragraph, the defendant

defendant, by his or her fault or his or her negligence, incapacitated him or herself of continuing to participate in the hearing (Article 332[62] (6) of the CPC). Or for cases where the defendant disrespects the court repeatedly throughout the session (Article 325[63] (4) of the CPC). In such cases, when the defendant comes back to the court room he or she needs to be informed of what happened in his or her absence, and therefore a summary of that is communicated to the defendant, otherwise the hearing will be void (Article 332[64] (7) of the CPC). The same happens if the trial involves several defendants and some are absent, as they come back they have to be informed in sum of what happened for the hearing not to be void (Article 343[65] (4) of the CPC).

Trial can proceed in the absence of the defendant when the defendant who was regularly noticed of the date, time and place of the court hearing does not show up and the court, after following all lawful attempts to guarantee his or her presence, does not perceive the defendant's presence from the beginning of trial as absolutely vital to the pursue of the material truth (Article 333[66] (1) of the CPC). If the reason for not being present at the court hearing is attainable, the judge might decide

---

moves away from the hearing room, it can continue until the end if the defendant has already been questioned and the court does not consider his presence indispensable, being for all purposes represented by the defender.

[62] idem

[63] Article 325 - **Situation and conduct duties of the accused** 1 - The accused, even if he is detained or imprisoned, attends the free hearing in his person, unless precautions are necessary to prevent the danger of escape or acts of violence. 2 - The accused detained or arrested is, whenever possible, the last to enter the hearing room and the first to be removed from it. 3 - The accused is bound by the same conduct duties that, under the terms of the previous article, are imposed on the people who attend the hearing. 4 - If, during the hearing, the accused fails to respect due to the court, he is warned and, if he continues to behave, he is ordered to be collected from any dependency of the court, without prejudice to the ability to appear at the last interrogation and to read the sentence and the duty to return to the room whenever the court deems it necessary. 5 - The defendant removed from the hearing room, under the terms of the previous number, considers himself present and is represented by the defender. 6 - The defendant's removal applies only to the session during which he has been ordered. 7 - The provisions of paragraph 3 of article 85 are correspondingly applicable.

[64] Above Footnote 61

[65] Above, Footnote 60

[66] Article 333 **Failure to attend and trial in absentia as regards the defendant duly served to appear** 1 - Where the defendant duly served to appear is not present at the hour fixed for the hearing to begin, the presiding judge takes the necessary and legally admissible measures in order to secure the defendant's appearance. The hearing shall not be adjourned unless the court considers that the defendant's presence since the beginning of the hearing is absolutely indispensable for the finding of the material truth. 2 - Where the court finds that the hearing may begin in the defendant's absence, or where the defendant's failure to attend is due to the reasons stated in article 117(2)(4), the hearing shall not be adjourned. Instead, the persons present thereto shall be heard pursuant to the order set forth in article 341(b)(c), notwithstanding any alteration deemed necessary to the list of witnesses previously produced. The witnesses' statements shall be recorded and the provisions of article 117(6) shall apply accordingly, where necessary. 3 - In the case referred to in the preceding paragraph, the defendant keeps his/her right to make statements until the closure of the hearing. If that takes place on the date initially fixed, the lawyer chosen by the defendant or the defence counsel appointed by the court may ask that the defendant be heard on the second date fixed by the judge pursuant to article 312(2). 4 – The provisions of the preceding paragraphs do not hinder the possibility for the hearing to take place in the defendant's absence upon his/her consent, according to article 334(2). 5 - In the case covered by paragraphs 2 and 3 above and where the hearing is to take place in the defendant's absence, the judgment handed down is served on the defendant immediately after his/her arrest or voluntary appearance. The deadline for an appeal to be lodged by the defendant is counted from the date of service of the judgement handed down. 6 – Through the service of the judgment upon the defendant, as foreseen in the preceding paragraph, the defendant is expressly informed of his/her right to appeal against the judgment, as well as of the deadline for lodging the appeal. 7 – The provisions of article 116(1)(2), of article 254 and of article 334(4)(5) shall apply accordingly.

(again, as the presence of the defendant is not considered utterly essential) to proceed with the court hearing and his or her legal counsel can request that the defendant is heard in the second court hearing before the end of trial (Article 333 (2) (3)[67] of the CPC). The presence of the legal counsel is always mandatory. In these cases, the final decision is noticed to the defendant upon his or her arrest or he or she voluntarily surrender (Article 333 (5)[68] of the CPC) and in this notice the defendant is informed of his or her right to appeal the decision and of the timeframe to do so (Article 333 (6)[69] of the CPC). The defendant is also informed of changes to the facts.

The final decision is read in court at the end of the hearing and the parties are considered noticed from then on (even the absent defendant, as he or she will be considered noticed through his or her legal counsel that is present), as established in Article 372[70] (3) (4) of the CPC. The judgment is deposited in writing at the court secretariat (Article 372 (5)[71] of the CPC).

The procedures described are form the common proceedings. Special proceedings forms have other particularities regarding namely timeframe but the information provided is the same.

b) The information above mentioned is provided orally by the judge (Article 343[72] (1) and Article 358[73] of the CPC). The court hearing is mandatorily recorded (Article 364[74] (1) of the CPC). The judgment is also written and made available at the court secretariat (Article 372[75] (5) of the CPC).

---

[67] idem
[68] Idem
[69] idem
[70] Article 372 - **Elaboration and signature of the sentence** 1 - After the deliberation and voting is concluded, the president or, if he is unsuccessful, the senior judge of those who make maturity, prepare the sentence according to the positions that have matured. 2 - Then, the sentence is signed by all the judges and the jurors and, if any of the judges signs expired, he / she declares precisely the reasons for his / her vote. 3 - When the court returns to the courtroom, the sentence is read publicly by the president or another judge. The reading of the report can be o mitted. The reading of the reasoning or, if it is very extensive, of its summary, as well as of the device, is mandatory, under penalty of nullity. 4 - The reading of the sentence is equivalent to its notification to the procedural subjects who must consider themselves present at the hearing. 5 - Right after reading the sentence, the president deposits it at the secretariat. The secretary sets the date, subscribes to the deposit statement and delivers a copy to the procedural persons who request it.
[71] Idem
[72] Footnote 60
[73] Article 358 - **Non-substantial change in the facts described in the indictment or in the indictment** 1 - If during the hearing there is a non-substantial change in the facts described in the indictment or in the indictment, if any, with relevance to the decision of the case, the president, of his own motion or upon request, communicates the change to the accused and grants him, if he so requests, the time strictly necessary for the preparation of the defense. 2 - Subject to the provisions of the preceding paragraph, the case of the alteration having resulted from facts alleged by the defense. 3 - The provisions of paragraph 1 are correspondingly applicable when the court changes the legal classification of the facts described in the indictment or in the indictment.
[74] Footnote 57
[75] Footnote 70

Regarding special procceedings, it is important to mention that in one of these special forms, the summary proceedings (processo sumário), the judgment is given orally and registered in the report of the hearing (acta), but the preferred means is also audio recording (Article 389-A[76] (1) (2) (3) of the CPC). A copy of the recording needs to be delivered to the defendant within 48 hours (Article 389-A (4)[77] of the CPC) and if the penalty is custodial then the judgement has to be written and read (Article 389-A (5)[78] of the CPC).

c) The information on the right to make statement and right to remain silent is provided at the beginning of the court hearing. The information on non-substantial changes to the accusation or decision by the examining magistrate in the instruction stage confirming the accusation is provided as soon as they are of the judge's knowledge at his or her own motion or at the request of the public prosecutor, the legal counsel or the legal representative of the 'assistant' (Article 358 (1)[79] of the CPC).

The right to be present in any procedural act that affects the defendant; right to be heard by a judge or examining magistrate when a decision that personally affects them is made; right to communicate in private with his or her legal counsel; right to provide evidence during the investigation and the instruction stages; right to be informed every time of his or her rights by the authority he or she will be heard (Article 61[80] of the CPC).

Right to information:

In the first judicial hearing of a detained defendant, the information is provided orally by the examining judge (Article 141[81] of the CPC).

[76] Article 389-A - **Sentence** 1 - The sentence is immediately rendered orally and contains: a) The summary indication of the proven and unproven facts, which can be made by reference to the accusation and contestation, with succinct indication and critical examination o f the evidences; b) A concise statement of the reasons of fact and of law that support the decision; c) In case of conviction, the succinct grounds that governed the choice and measure of the sanction applied; d) The device, under the terms provided for in paragraphs a) to d) of paragraph 3 of article 374. 2 - The device is always dictated for the minutes. 3 - The sentence is, under penalty of nullity, documented under the terms of articles 363 and 364. 4 - A copy of the recording is always delivered to the accused, the assistant and the Public Prosecutor's Office within 48 hours, unless those expressly declare to waive delivery, without prejudice to any procedural subject to be able to request under the terms of paragraph 4 of article 101. 5 - If a custodial sentence is applied or, exceptionally, if the circumstances of the case make it necessary, the judge , right after the discussion, draw up the sentence in writing and read it.
[77] idem
[78] idem
[79] Above, footnote 73;
[80] Footnote 46, above;
[81] Footnote 51, above.

It can also be provided for to the defendant under custody by the public prosecutor in a first non-judicial questioning of the defendant under custody (Article 143[82] of the CPC).

During trial, after the introductory acts, the judge briefly exposes the object of the proceedings by reading the accusation (or decision by the examining magistrate in the instruction stage confirming the accusation) where the facts hold against the defendant are included, in the presence of the defendant (Article 339[83] of the CPC) or, in his or her absence, of the legal counsel (Article 333[84] and 334[85] of the CPC).

Defendants are informed of the facts that are hold against them, including circumstances of place, time and manner, if these are known.

During investigation stage, and when a defendant is not under custody, interrogation is made by the public prosecutor or the criminal police authority and the defendant is informed of his or her procedural rights (Article 61[86] of the CPC) and of the facts that are hold against him or her, including circumstances of place, time and manner, if these are known (Article 141 (4) a) and d)[87]

---

[82] Article 143 **First out-of-court preliminary questioning of an arrested defendant** 1 – The arrested defendant who is not examined by the Examining Judge immediately after his/her arrest shall be brought before the competent public prosecutor of the area where the arrest took place and the public prosecutor shall then hear him/her briefly. 2 – The questioning shall abide, in the applicable part, by the provisions relating to the first preliminary court examination of an arrested defendant. 3 – After the brief questioning, the public prosecutor, should he not release the person arrested, shall take the necessary steps so that the defendant may be brought before the Examining Judge pursuant to articles 141 and 142. 4 – In cases of terrorism, violent or highly organized crime, the public prosecutor may prevent the person arrested from having contacts with persons other than his/her defense counsel, before the first preliminary court examination.

[83] Article 339 - **Introductory presentations** 1 - After the introductory acts referred to in the preceding articles have been carried out, the president orders the removal of the room from the persons who must testify, and he can proceed in the same way in relation to other persons who must be heard, and makes a brief presentation. about the subject of the process. 2 - The President then gives the floor, in the order indicated, to the Public Prosecutor's Office, to the attorneys of the assistant, the injured party and the civil responsible and the defender, so that each of them can indicate, if he so wishes, summarily and within ten minutes, the facts you propose to prove. 3 - The president actively regulates the exposures referred to in the preceding paragraph, in order to avoid ramblings, repetitions or interruptions, as well as to make them become preliminary allegations. 4 - Without prejudice to the regime applicable to the alteration of the facts, the discussion of the case has as its object the facts alleged by the prosecution and the defense and those resulting from the evidence produced in the hearing, as well as all the relevant legal solutions, regardless of the legal qualification of the facts resulting from the accusation or pronouncement, in view of the purposes referred to in articles 368 and 369.

[84] Footnote 66, above;

[85] Article 334 - **Hearing in the absence of the defendant in special cases and of public notice** 1 - If the case is subject to a very brief process but the procedure has been forwarded to the common form and if the defendant cannot be notified of the order that designates the day for the hearing or absences from the hearing unjustifiably, the court may order the hearing to take place in the absence of the accused. 2 - Whenever the defendant is practically unable to attend the hearing, namely due to age, serious illness or residence abroad, he may request or consent to the hearing taking place in his absence. 3 - In the cases provided for in paragraphs 1 and 2, if the court considers the presence of the defendant to be absolutely indispensable, order it, interrupting or postponing the hearing, if necessary. 4 - Whenever the hearing takes place in the absence of the accused, the defendant is represented, for all possible purposes, by the defender. 5 - In case of connection of cases, the defendants present and absent are judged jointly, unless the court has the most convenient separation of cases. 6 - Outside the cases provided for in paragraphs 1 and 2, the sentence is notified to the defendant who was judged to be absent as soon as he is detained or voluntarily presents himself. The deadline for filing an appeal by the accused is counted from the notification of the sentence. 7 - In the notification provided for in the preceding paragraph, the accused is expressly informed of the right to appeal the sentence and the respective term. 8 - The provisions of paragraphs 1 and 2 of article 116 and article 254 are correspondingly applicable.

[86] above

[87] above

of the CPC); and when the defendantis arrested he or she will furthermore be informed of the reasons for the detention (Article 141 (4) c) [88]of the CPC). The information regarding the facts hold against the defendant is provided orally but is written down in the interrogation report.

When a coercive measure is ordered against the defendant, the decision that determines it is noticed in writing to the defendant and the decision contains (otherwise it is void) the description og the concrete facts the defendant is suspected of having committed, including, whenever possible, the circumstances of place, time and manner (Article 194[89] (6) a) and (9) of the CPC).

Once the investigation stage ends the accusation is written down with narration of the facts that reason the propose the application of a given penalty, including, if possible, stating the circumstances of place, time and manner of the crime and the degree of participation the defendant had in it and any circumstances that were relevant to determine the particular penalty entailed (Article 283[90] (3) of the CPC). This written decision is noticed to the defendant and his or her legal

[88] above

[89] Article 194 **Hearing of the defendant and court order imposing a coercive or patrimonial guarantee measure** 1 – With the exception of the Statement of Identity and Residence, the coercive and patrimonial guarantee measures shall be imposed by means of an order is sued by the Examining judge, either during the inquiry and upon request of the Public Prosecution Service or after the inquiry ex officio, once the public prosecutor has been heard on the matter, under penalty of nullity. 2 – During the inquiry, the judge may impose a coercive measure other than the one requested by the public prosecutor, even if heavier in terms of nature, length or manner of enforcement, on the grounds of the provisions laid down in article 204(a)(c). 3 – During the inquiry, the judge may not impose a heavier coercive measure, in terms of nature, length or manner of enforcement, on the grounds of the provisions laid down in article 204(b), nor can he impose a patrimonial guarantee measure heavier than the one requested by the public prosecutor, under penalty of nullity. 4 – The imposition of the measures provided for in paragraph 1 above is preceded by the hearing of the defendant, except for those cases in which an impediment is duly substantiated, and may take place during the first preliminary court examination, being the provisions set forth in article 141(4) always applicable to the hearing of the defendant. 5 – During the inquiry, except where there is a duly substantiated impossibility, the judge shall decide whether or not to impose a coercive or patrimonial guarantee measure on a defendant who is not under arrest within five days following the receipt of the public prosecutor's request. 6 – The substantiation of the order by means of which any coercive or patrimonial guarantee measure is imposed, with the exception of the Statement of Identity and Residence, shall contain, under penalty of nullity: a) A description of the specific facts of which the defendant stands accused, including, if known, the circumstances of time, place and method; b) A statement of the elements contained in the case file which evidence the charges brought against the defendant, whenever the communication of such elements does not seriously jeopardize the investigation, does not hamper the discovery of the truth and does not endanger the life, the physical or psychological integrity or the freedom of the parties to the case or of the victims of the crime; c) The legal qualification of the facts of which the defendant stands accused; d) A reference to the specific facts which meet the requirements for the imposition of the measure, including those foreseen in articles 193 and 204. 7 – Without prejudice to subparagraph b) of the preceding paragraph, facts or elements contained in the case file but not communicated to the defendant during the hearing mentioned in paragraph 3 above shall not be taken into account when substantiating the imposition of a coercive or patrimonial guarantee measure on the defendant, with the exception of the Statement of Identity and Residence. 8 – Without prejudice to subparagraph b) of paragraph 6 above, both the defendant and his /her defence counsel may be granted access to the elements contained in the case file which are instrumental to the imposition of the coercive or patrimonial guarantee measure, with the exception of the Statement of Identity and Residence, during the preliminary court examination and within the period of time provided for the lodging of an appeal. 9 – The order to which mention is made in paragraph 1 above, containing a warning regarding the consequences of non-compliance with the obligations imposed, is served on the defendant. 10 – In case of remand in custody, the order is immediately communicated to the defence counsel and, whenever the defendant so wishes, to a relative or person of his/her trust.

[90] Article 283 **Bill of indictment produced by the Public Prosecution Service** 1 - Where enough evidence regarding the commission of a criminal offence and allowing the identification of the defendant has been gathered during the inquiry, the Public Prosecution Service has a 10-day period to produce a bill of indictment against the said defendant. 2 - Sufficient evidence is the evidence on the basis of which it is reasonable to believe that a sentence or a security measure would be imposed on the defendant should he/she face trial. 3 - The bill of indictment must contain the following

counsel (Article 283 (5)[91] and Article 277 (3)[92] of the CPC). It is communicated either by registered post or in person (Article 283 (6)[93] of the CPC).

When the instruction stage is initiated, and until the end of it, if there is enough evidence that the assumptions determining the application of a given penalty are met, the examining magistrate, in a written decision, confirms the accusation (Article 308[94] CPC). This decision again contains the facts the defendant is hold for. This decision is noticed to the defendant.

The victim

information, otherwise it shall be deemed null and void: a) The particulars of the defendant; b) The summary of the facts causing the imposition on the defendant of a sentence or of a security measure, including, where possible, the place, time and grounds for the commission of the offence, the degree of the defendant's involvement thereon and the circumstances relevant to the determination of the sanction to apply; c) Reference to the applicable legal provisions; d) A list of 20 witnesses maximum and their particulars, with specification of those witnesses – in a number not exceeding five – who are to give evidence regarding the facts mentioned in article 128(2); e) The names of experts and technical advisors to be heard during trial and their respective particulars; f) Reference to any other means of evidence to be produced or requested; g) The date and signature. 4 - Should different case proceedings become one, only one bill of indictment shall be produced. 5 - The provisions set forth in article 277(3) shall apply accordingly, and the proceedings shall be continued whenever the notification procedures have proved to be ineffective. 6 - The communications referred to in the preceding paragraph are made through personal service or by registered mail, except where the defendant and the party assisting the Public Prosecutor have communicated their place of residence or professional domicile to the police or judicial authority in charge of issuing the offence report minutes or of taking their statements during either the inquiry or the preliminary judicial stage. In this case, they shall be served by standard mail pursuant to article 113(1)(c). 7 - The limit of witnesses set forth in paragraph 3, sub-paragraph d) hereinabove may be surpassed if deemed necessary for purposes of ascertaining the truth, in particular whenever an offence covered by article 215(2) has been committed or the proceedings prove to be exceptionally complex due to the number of defendants and victims involved or due to the highly organized nature of the criminal offence. In the request submitted, mention must be made to the facts about which witnesses shall testify and the reason why such witnesses have a direct knowledge of those facts. 8 – The request referred to in the preceding paragraph shall be rejected where the circumstances foreseen in article 340(4)(b)(c)(d) arise.

[91] Id.

[92] Article 277 - **Archiving of the investigation** 1 - The Public Prosecutor proceeds, by order, to archive the investigation, as soon as he has collected enough evidence that he has not verified a crime, that the accused has not committed it in any way or that he is legally the procedure is inadmissible. 2 - The investigation is also closed if it has not been possible for the Public Prosecutor to obtain sufficient evidence of the crime or who the agents were. 3 - The order for filing is communicated to the accused, the assistant, the whistleblower with the power to become an assistant and to anyone who has expressed the purpose of deducting a claim for civil compensation under the terms of article 75, as well as the respective defender or lawyer . 4 - The communications referred to in the previous number are made: a) By notification by personal contact or by registered post to the assistant and the defendant, unless they have indicated a specific place for the purposes of notification by simple post, in pursuant to paragraphs 5 and 6 of article 145, paragraph 2 and paragraph c) of paragraph 3 of article 196, and have not meanwhile indicated another one, by means of an application delivered or sent by registered post to the secretariat where the records are currently running; b) By public notices, if the defendant does not have an appointed defender or lawyer, and it is not possible to notify him through personal contact, by registered or simple post, as provided for in the preceding paragraph; c) By notification by simple post to the whistleblower with the option of becoming an assistant and to anyone who has expressed the purpose of deducting a claim for civil compensation; d) By notification by simple postal service whenever the investigation does not run against a specific person. 5 - In the cases provided for in paragraph 1, whenever it is found that the person who reported or exercised an alleged right of complaint existed, an abuse of the process, the court condemns him to pay a sum between 6 UC and 20 UC without prejudice to the determination of criminal liability.

[93] Footnote 90, above

[94] Article 308 - **Order of pronunciation or non-pronunciation** 1 - If, until the end of the investigation, sufficient evidence has been collected of having verified the assumptions on which the application of the penalty to the accused depends on security, the judge, by order, pronounces the accused by the respective facts; otherwise, it issues a non-pronunciation order. 2 - The provisions of article 283, paragraphs 2, 3 and 4 are correspondingly applicable to the order referred to in the preceding paragraph, without prejudice to the provisions of the second part of paragraph 1 of the previous article. 3 - In the order referred to in paragraph 1, the judge begins by deciding all previous or incidental issues that he may be aware of. 4 - In the order of pronouncement, the judge may request the elaboration of a social report or the updating of what is already in the process, to be presented until the moment when the sanction is determined, if deemed convenient in view of the subsequent judgment.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

The protection of victims of crime is inherent to the rule of law and, "the State is responsible, not only to" respect "fundamental rights and freedoms, but also" to guarantee their effectiveness ". Thus, immediate protection of fundamental rights, such as the right to life, physical integrity, privacy and property in the face of the danger of their injury (primary victimization), as well as mediate protection of the fundamental rights of others, is essential. entities, indirectly affected (secondary victimization).

This right of protection for victims is immediately reflected in the victim's right of access to the courts, and in the right of the victim to intervene in criminal proceedings. As for the latter, GOMES CANOTILHO AND VITAL MOREIRA draw attention by stating that, “unlike what happens in relation to the accused, the constitutional law does not specify the fundamental dimensions of the victim's right to intervene in the process, referring to the law that task”.

In the light of the current criminal procedural legislation, there are several competences made available to the victim, who is constituted as an assistant: to intervene in the investigation and in the investigation, offering evidence and requesting necessary steps, to deduct the accusation, to appeal against decisions that affect his interests.

Particular attention is drawn to the obligation for the victim to be an assistant in crimes dependent on private prosecution. To this end, the victim must be warned of this obligation by the criminal police body to whom the complaint is made verbally.

The Portuguese legislature, in harmony with the Constitution of the Portuguese Republic, sought to continue a criminal political program aimed at the victim of crime. Therefore, several protection measures were promoted, which we highlight:

- The duty of information, on the part of the judicial authorities and criminal police bodies, to any injured parties, about the possibility of deducting a request for civil compensation in criminal proceedings and the formalities to be observed.

- The possibility for the assistant, if he believes that advertising is harmful to him, to request the investigating judge to subject the case, during the investigation phase, to a secret of justice, as well as request its removal at any time during the investigation.

- The media is prohibited from transmitting or registering images, or sound recordings, relating to the practice of any procedural act, namely the hearing, unless judicial authorization, however, if the person opposes it, cannot be authorized to transmit or register images or sound taps related to your person; it is also forbidden to publish, by any means, the identity of the victims of crimes of trafficking in persons, against sexual freedom and self-determination, the honor or reserve of private life, unless the victim expressly consents to the disclosure of his identity or if the crime is committed through the media.
- The possibility of the judge, in case there is strong evidence of a criminal offense punishable by a maximum prison sentence of more than 3 years, to prohibit the accused from contacting the victim by any means.

Witnesses

Witnesses are entitled to witness protection – if necessary: Image hiding or voice distortion and teleconferencing; Identity reservation;. Witnesses are also eligible for pecuniary compensation for the time they were present before court. Witnesses are not obliged to answer any questions that might incriminate oneself. The witness is allowed to be acompainged by a lawyer in all stages of the proceedings where is called to intervene ( Article 132 CPC)[95].

5.1 The Prosecution

***56.* Question:** *Are there any requirements or guidance provided to the prosecution as how to control and deal with mobile forensics and evidences?*

No.

[95] Article 132 **Rights and duties of witnesses** 1 – Except as otherwise provided for by law, every witness has the duty to: a) Appear, at the right time and venue, before the authority having legitimately summoned or notified the witness, and to remain available until released; b) Giving oath, when heard by a judicial authority; c) Observing any indications legitimately given on how testimony should be given; d) Answer truthfully on questions addressed. 2 – A witness is not compelled to reply any questions when alleging that his replies might lead to his prosecution. 3 – In order to be notified, the witness may indicate his residence, workplace or another address of his choice. 4 – When requested to testify, even during an act forbidden to the public, a witness may be accompanied by a lawyer who is bound to inform him, if necessary, on his rights, without intervening in the interview. 5 – A lawyer assisting a defendant in criminal proceedings may not accompany a witness under paragraph 4 above.

5.2 The Court

***57.* Question:** *Is there judicial control over the approaches and methods used for acquiring, collecting and analyzing evidence? Please refer to case law if possible.*

Yes. Rules on approaches and methods used for acquiring, collecting and analyzing evidence can be found in the CPC in Article 127[96]- Free assessment of evidence; Articlea 151 to 163[97] – Expert Forensic evidence; Articles 164 to 170[98] documental means of evidence; Articles 171 to 186[99] on means of acquiring and collecting evidence ( in general) and; Articles 187 to 190[100] regarding phone tapping.

[96] Article 127 - **Free assessment of evidence** Except when the law provides otherwise, the evidence is assessed according to the rules of experience and the free conviction of the competent entity.

[97]

[98]

[99]

[100] Article 187 **Admissibility** 1 - Interception and tape recording of telephone conversations or communications may only be authorized during the inquiry where there are grounds for believing that this step is indispensable for the discovery of the truth or that the evidence would, by any other means, be impossible or very hard to collect. Such authorization shall be granted by means of a reasoned order issued by the Examining Judge and upon the request of the Public Prosecution Service, as regards the following criminal offences: a) Criminal offences to which a custodial sentence with a maximum limit over three years applies; b) Drug-related offences; c) Possession of a prohibited weapon and illicit trafficking in weapons; d) Smuggling offences; e) Insult, threat, coercion, disclosure of private life and disturbance of the peace and quiet, whenever committed by means of a telephone device; f) Threat with the commission of a criminal offence or abuse and simulation of danger signals; or g) Escape from justice, whenever the defendant has been sentenced for a criminal offence foreseen in the preceding sub-paragraphs. 2 – The authorization provided for in paragraph 1 above may be requested to the judge with jurisdiction over the locations from where the telephone conversation or communication is likely to be effected, or over the central office of the entity competent to conduct the criminal investigation, when dealing with the following criminal offences: a) Criminal offences to which a custodial sentence with a maximum limit over three years applies; b) Illegal restraint, kidnapping and taking of hostages; c) Offences against cultural identity and personal integrity, as provided for in Book II, Title III, of the Criminal Code and in the Criminal Law on Violations of International Humanitarian Law; d) Offences against State security foreseen in Book II, Title V, Chapter I, of the Criminal Code; e) Counterfeiting of currency or securities equivalent to currency foreseen in articles 262, 264 - to the extent that it refers to article 262- and article 267 – to the extent that it refers to articles 262 and 264 - of the Criminal Code; f) Offences covered by a convention on the safety of air or maritime navigation. 3 – In the cases foreseen in the preceding paragraphs, the authorization is communicated within a seventy-two hour period to the judge to whom the case was referred, who is responsible for carrying out the subsequent jurisdictional acts. 4 - Regardless of the entity who owns the means of communication used, both the interception and the recording referred to in the preceding paragraphs can only be authorised against: a) The suspect or the defendant; b) Any person acting as an intermediary, against whom there are grounds to believe that he/she receives or transmits messages aimed at, or coming from, the suspect or the defendant; or c) A victim of a crime upon his/her effective or alleged consent. 5 - No interception and recording of telephone conversations or communications between the defendant and his defence counsel is allowed unless the judge has reasonable grounds to believe that the said conversation or communication is the object or the constitutive element of a criminal offence. 6 - The interception and the recording of any conversations or communications are authorised for a maximum time-limit of three months, renewable for equal periods, provided that the respective requirements for admissibility have been met. 7 - Without prejudice to article 248, the recording of conversations or communications cannot be used in the scope of any other proceedings, either on-going or to be instituted, unless it has resulted from the interception of a means of communication used by the person referred to in paragraph 4 above and insofar as it proves to be indispensable for obtaining evidence of the crime set out in paragraph 1 above. 8 - In the cases provided for in paragraph 7 above, the technical means in which conversations or communications have been recorded, as well as the decisions having clearly stated the need for the interceptions are enclosed, following a judge's ruling, to the proceedings in the scope of which they are to be used as evidence. If necessary, copies thereof shall be made.
Article 188 **Formalities of the operations** 1 – The criminal police body carrying out the interception and the recording referred to in the preceding article draws up the respective records and produces a report pointing out the parts which bear relevance to the evidence, describing in brief the respective contents and explaining the respective importance for the discovery of the truth. 2 – The provisions set forth in the preceding paragraph

***58.* Question:** *How does the Court assess the evidence obtained via mobile forensics? Please refer to case law if possible to illustrate the approach.*

There are no specific rules regarding assessement of evidence obtained via mobile forensics. General rules on the assessment of evidence apply.

5.3 The defendant and defender

***59.* Question:** *Are there rules and standards regulating the defendant and his/her defender's rights to access and to make copies of the acquired mobile evidence? Are they able to get any information on the process used to acquire mobile forensic evidence (e.g. information on how*

---

do not prevent the criminal police body responsible for the investigation from having previous knowledge of the contents of the intercepted communication in order to perform the investigative steps deemed necessary and urgent for purposes of ensuring any means of evidence. 3 – The criminal police body mentioned in paragraph 1 above provides the Public Prosecution Service, every fortnight counted from the first interception made, with the respective technical material, as well as with the respective records and reports. 4 – The Public Prosecution Service submits the elements mentioned in the preceding paragraph to the judge within a maximum time limit of forty-eight hours. 5 – In order to become acquainted with the content of the conversations or communications, the judge shall be assisted, whenever appropriate, by a criminal police body and shall appoint, if necessary, an interpreter. 6 – Without prejudice to the provisions set forth in paragraph 7 of the preceding article, the judge shall order the immediate destruction of the technical materials and reports clearly bearing no interest to the case at hand: a) Concerning conversations between persons not referred to in paragraph 4 of the preceding article; b) Covering matters under professional secrecy, under secrecy binding officials or under State secrecy; or c) The disclosure of which may seriously affect rights, liberties and guarantees; and all interveners in the operations shall be bound by the duty of secrecy as to what has been disclosed through the said conversations. 7 – During the inquiry, the judge shall order, upon the request of the Public Prosecution Service, the transcription into and annexation to the proceedings of the conversations and communications which, on solid grounds, justify the application of coercive or patrimonial guarantee measures, with the exception of the Statement of Identity and Residence. 8 – Upon conclusion of the inquiry stage, both the party assisting the Public Prosecutor and the defendant may accede to the technical materials of the conversations or communications and obtain, at their own expense, copies of the parts which they intend to transcribe for purposes of annexation to the case, as well as of the reports foreseen in paragraph 1 above, until the expiry of the time-limits given for purposes of requesting the opening of the preliminary judicial stage or for purposes of producing the defense statement. 9 – Conversations or communications that can be used as evidence are only those which: a) The Public Prosecution Service orders the criminal police body responsible for the interception and recording to transcribe and which have been pointed out in the indictment as being means of evidence; b) The defendant transcribes from the copies foreseen in the preceding paragraph and encloses to the application for the opening of the preliminary judicial stage or to the production of the defense statement; or c) The party assisting the Public Prosecutor transcribes from the copies foreseen in the preceding paragraph and encloses to the case within the time limit foreseen for requesting the opening of the preliminary judicial stage, even if such a party does not request the said opening or has no legitimacy to do so. 10 – The court may hear the recordings so as to determine the correction of the transcriptions already made or the respective annexation to the proceedings of new transcriptions, whenever needed for purposes of discovering the truth and of giving a just decision on the case. 11 – The persons whose conversations or communications have been heard and transcribed may examine the respective technical materials until the closure of the trial hearing. 12 – The technical materials concerning conversations or communications which are not transcribed for purposes of being used as means of evidence are kept inside sealed envelopes, upon an order by the court, and destroyed after the decision on the case has acquired legal force. 13 – After the decision has become final, as mentioned in the preceding paragraph, the technical materials which have not been destroyed shall be kept inside a sealed envelope, enclosed to the proceedings, and may only be used should an extraordinary appeal be lodged.

Article 189 **Scope** 1 – The provisions laid down in articles 187 and 188 shall apply accordingly to any conversation or communication transmitted through any technical means other than a telephone device, in particular by e-mail or other forms of telematics data transmission, even if kept under a digital medium, and to the interception of the communications between persons present. 2 – Obtaining and enclosing to the proceedings data regarding mobile phone tracing or records of conversations or communications may only be ordered or authorized, regardless of the stage of the proceedings, by means of an order issued by the judge, as regards criminal offences foreseen in article 187(1) and the persons mentioned in article 187(4).

Article 190 **Nullity** The requirements and conditions referred to in articles 187, 188 and 189 are established under penalty of nullity.

*the tools work, the procedures used, the parties involved and how the validity of the results is guaranteed)? Please refer to case law if possible.*

This question is answered in question 55.

5.4 Witnesses

***60.* Question:** *During the pre-trial stage, how is the right to privacy of the witnesses preserved? Are there any practical steps taken to exclude certain types of information which are cumulatively non-relevant to the case and too private? Are there particular requirements for witnesses regarding their capability to testify in terms of mobile forensics both in the pre-trial and the trial phase of the criminal proceedings? Please refer to case law if possible.*

This question is answered in question 55.

5.5 The Victim

***61.* Question:** *How are the victim's/victims' rights ensured during both the pre-trial and the trial phase of the proceedings? How is their privacy preserved? Can they use the evidence obtained via mobile forensics when exercising their rights? Please refer to case law if possible.*

This question is answered in question 55.

**Section 6: Comments**

*If you feel some important elements of your national law relating to the use of mobile forensics in criminal investigations have not sufficiently been covered, please explain them here. If you feel an overview is missing, please also provide guidance on this below.*

**Answer:** Indication of length of answer: few paragraphs up to a couple of pages.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter – @Formobile2019
www.formobile-project.eu

*Bibliography*

ANTUNES, Maria João - *Direito Processual Penal.* Lisboa: Almedina, 2017. ISBN978-972-40-6558-8

CANOTILHO, José Joaquim Gomes; MOREIRA, Vital - *Constituição da República Portuguesa Anotada Artigos 1º a 107º*. Coimbra: Coimbra Editora, 2007. ISBN 978-972-32-1462-8

CANOTILHO, José Joaquim Gomes; MOREIRA, Vital - *Constituição da República Portuguesa Anotada, Volume II, Artigos 108º a 296º, 4ª edição*. Coimbra: Coimbra Editora, 2014. ISBN 978-972-32-2287-6

SILVA, Germano Marques da - *Direito Processual Penal Português: Do Procedimento (Marcha do Processo)*. Lisboa: Universidade Católica Editora, 2018. ISBN 9789725404270

TRIUNFANTE, Luís de Lemos – Admissibilidade e validade da prova na Decisão Europeia de Investigação, *JULGAR online*, abril de 2018.