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: bpv Grigorescu-Stefanica and Associates (Law firm), Octavian Marian Senior Associate Lawyer.

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

Answer: Bucharest, Romania.

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, there is no legal definition for "*mobile device*".

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

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?*

Answer: The Romanian Criminal Procedure Code (hereinafter "***CPC***") provides the conditions under which a mobile device can be read or searched without a seizure. Thus, the provision of article 138 of CPC regulates the following relevant electronic surveillance methods which can be used by the criminal investigation bodies:

a) **wiretapping of communications or of any type of remote communication**;
   - *"Wiretapping of communications or of any type of messages designates the wiretapping, accessing, monitoring, collection or recording of communications via phone, computer system or any other communication device."*[1]

b) **accessing an informatics systems;**
   - *"Accessing an informatics system designates the penetration of an informatics system or of other data storage device either directly or from a distance, through specialized programs or through a network, for the purpose of identifying evidence;"*[2]

[1] Article 138 para. (2) of CPC
[2] Article 138 para. (3) of CPC

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

- *An informatics system is any device or combination of devices interconnected between them or in a functional relationship, one or more of which provide the automatic data processing by means of a computer program;*[3]

According to the provisions of article 139 of CPC, the above electronic surveillance methods can be read or searched without seizure of the mobile device only if the following requirements are **cumulatively** met:

a) there is reasonable suspicion concerning the preparation or commission of one of the following criminal offences: offences against national security stipulated by the Criminal Code and by special laws, as well as in case of drug trafficking, illegal operations with precursor or other products likely to have psychoactive effects, offences related to non-compliance with the regime of weapons, ammunition, nuclear materials, explosives and restricted explosive precursors, trafficking and exploitation of vulnerable persons, acts of terrorism, money laundering, counterfeiting of coins, stamps or other valuables, counterfeiting of instruments electronic payment, in the case of crimes committed through computer systems or electronic means of communication, against property, blackmail, rape, unlawful deprivation of liberty, tax evasion, corruption offences and offences assimilated to corruption, offences against the European Union's financial interests, offences committed by means of computer systems or electronic communication devices, or in case of other offences in respect of which the law sets forth a penalty of no less than 5 years of imprisonment;

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

[3] Article 138 para. (4) of CPC

c) evidence could not be obtained in any other way or its obtaining implies special difficulties that would harm the investigation, or there is a threat for the safety of persons or of valuable goods;

The electronic surveillance methods may be ordered by the Judge for rights and liberties only if a criminal investigation is undergoing, for a term of maximum 30 days and only upon request of the prosecutor. Such application filed by the prosecutor has to contain: the electronic surveillance measures that are requested for authorization, the name or the identification data of the person against whom such measure is to be ordered, if known, the evidence or data giving rise to a reasonable suspicion related to the commission of an offence in respect of which such measure may be ordered, the facts and the charges and a justification of the proportional and subsidiary nature of the measure. The prosecutor has to submit the case file to the Judge for rights and liberties. In case of offences against national security, the warrant is issued by a specially appointed judge from The High Court of Cassation and Justice according to the provisions of Law no. 51/1991 on the national security of Romania.

Also, please note that by exception, the prosecutor may authorize, for a time period of maximum 48 hours, the electronic surveillance methods if: a) there is an emergency situation, and the obtaining of an electronic surveillance warrant from the Judge for rights and liberties would lead to a substantial delay of investigations, to the loss, alteration or destruction of evidence, or would jeopardize the safety of the victim, of witnesses or of their family members; and b) the requirements mentioned above (i.e. letter a) – c) are met. Within a maximum of 24 hours following the expiry of a measure, the prosecutor is under an obligation to notify the competent Judge for rights and liberties of the court to confirm the measure and, at the same time, shall forward a report presenting a summary of the electronic surveillance activities performed and the case file.

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?*

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

Answer: Search of the mobile device should be limited to those aspects related to the investigated crime. The warrant ordered by the Judge of rights and liberties should contain the identification elements of the mobile device (e.g. name, model, International Mobile Equipment Identity – IMEI etc.). The CPC does not offer supplementary instructions regarding the limits of the search. However, the provisions of article 142 para. (1^1) of CPC, regulates that the criminal bodies shall directly use the appropriate technical systems and procedures, such as to ensure the integrity and confidentiality of the data and information collected. Moreover, the criminal bodies should take action in order to ensure that the search is conducted without making facts and circumstances of the private life of the person subject to search, public in an unjustified manner. Finally, the electronic surveillance of the relationship between the lawyer and the client is not permitted, unless there is information that the lawyer perpetrates or prepares the commission of any of the offences listed above at the question no. 4.

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

Answer*:* Yes, article 136 para. (3) of CPC expressly indicates that the access can be made through specialized programs. In practice the Romanian criminal bodies use the following programs: Encase forensic, Magnet Axiom Computers, Oxygen Forensic Detective, Cellebrite UFED 4PC Ultimate UFED4PC Ultimate Kit).

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

Answer*:* Yes, the information can be copied. Analysing the definition of the two electronic surveillance methods mentioned above, we observe that the law indicates the possibility to "*collect*" the information.

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

Answer: No consent is needed.

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

Answer: No, he/she cannot be forced to unlock the mobile device.

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

Answer: Yes, according to the provision of article 145 of CPC, following termination of electronic surveillance of the mobile device, the prosecutor shall inform each subject of the warrant for electronic surveillance enforced against them, in writing, within maximum 10 days. Following such information, a person subject to surveillance has the right to learn, upon request, of the content of the minutes recording the electronic surveillance activities performed. Also, the prosecutor has to ensure, upon request, the listening of the discussions, communications or conversations, resulted from each electronic surveillance activity.

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

Answer: Please observe our answer from question no.4.

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

Answer: The provisions of the CPC does not expressly specify who can be subject to the surveillance methods. However, based on the interpretation of the law and on our previous experience and practice, we mention that even a third party or a witness can be subject to surveillance.

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.*

Answer: The provision of the CPC does not regulate such situation. However, on article 548 of CPC it is mentioned that international judicial cooperation shall be requested or granted in compliance with the stipulations of the legal acts of the European Union, the international treaties for international judicial cooperation that Romania is a party. Also, it is established that acts performed by seconded foreign members of a joint investigative team on the basis of and in

compliance with the orders of the team leader shall carry similar value to those performed by the Romanian criminal investigation bodies.

Thus, bearing in mind the provision of article 548 of CPC, in such cases the criminal investigation bodies will request an EIO based on the provision of Law no. 302/2004 regarding international judicial cooperation in criminal investigation which has transposed the provisions of the Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters.

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

Answer: Yes, the electronic surveillance methods can be used by the criminal investigation bodies only if there is an undergoing criminal investigation regarding the following types of criminal offences: offences against national security stipulated by the Criminal Code and by special laws, as well as in case of drug trafficking, illegal operations with precursor or other products likely to have psychoactive effects, offences related to non-compliance with the regime of weapons, ammunition, nuclear materials, explosives and restricted explosive precursors, trafficking and exploitation of vulnerable persons, acts of terrorism, money laundering, counterfeiting of coins, stamps or other valuables, counterfeiting of instruments electronic payment, in the case of crimes committed through computer systems or electronic means of communication, against property, blackmail, rape, unlawful deprivation of liberty, tax evasion, corruption offences and offences assimilated to corruption, offences against the European Union's financial interests, offences committed by means of computer systems or electronic communication devices, or in case of other offences in respect of which the law sets forth a penalty of no less than 5 years of imprisonment.

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.*

Answer: According to the article 102 of CPC, evidence obtained unlawfully may not be used in criminal proceedings. Also, please note that the nullity of the document which ordered the

electronic surveillance methods of the mobile device, triggers the exclusion of the obtained evidence. In addition, derived pieces of evidence are excluded if these were obtained directly from evidence obtained unlawfully and could not be obtained in another way.

However, we outline that not any violation of the legal provisions excludes the evidence, but only those that represent a substantial and significant violation of the CPC provisions or of the special legislation governing the administration of evidence, if by this violation the fairness of the criminal process is achieved by damaging the rights of the parties and which cannot be removed otherwise or which may raise serious doubt as to the reliability of the evidence.

The judge will be the one who will appreciate if the breach of the law determined the violation of the fundamental rights of the parties and affected the fairness of the criminal trial. In such case, even if the document which order the electronic surveillance (the warrant) is not affected by nullity, the evidence should be inadmissible. Certainly, if the document which order the electronic surveillance will be affected by nullity then always the evidence will be considered inadmissible.

Mobile device seized

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

Answer*:* Yes, separately of the above electronic surveillance methods which do not include the seizure of the mobile device, the provisions of the CPC gives the possibility to search a mobile device with the seizure of these. As per the provisions of article 168 of CPC, an electronics system search or a data storage medium search designates the procedure for the investigation, discovery, identification and collection of evidence stored in an electronics system or in a data storage medium, performed by means of adequate technical devices and procedures, of nature to ensure the integrity of the information contained by these.

If the person is not accused nor defendant and there is reasonable suspicion in relation to the preparation or commission of a criminal offence and there are reasons to believe that an object (such as a mobile device) can serve as evidence in a case, the criminal investigation bodies or the

court may order the natural person or legal entity holding the mobile device, to provide and surrender, subject to receiving proof of surrender. Also, if the above requirements are met, the criminal investigation bodies or the court may order:

a) any natural person or legal entity on the territory of Romania to communicate specific informatics data in their possession or under their control that is stored in a mobile device;
b) any provider of public electronic communication networks or provider of electronic communication services intended for the public to communicate specific data referring to subscribers, users and to the provided services that is in its possession or under its control, other than the content of communications.

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

Answer: During the criminal investigation, the competent Judge for rights and liberties may order the conducting of a search, upon request by the prosecutor, when the investigation of a mobile device is necessary for the discovery and collection of evidence. The prosecutor shall submit an application requesting the approval of an electronics search together with the case file to the Judge for rights and liberties.

During the trial, the search of the mobile device is ordered by the court, ex officio or upon request by the prosecutor, by the parties or the victim.

After the search of the mobile device is finalised, the criminal investigation bodies are obliged to draft a report which should contain: a) name of the person from whom the mobile device is seized or name of the person whose mobile device is subject to search; b) name of the person having conducted the search; c) names of the persons present during the search conducting; d) a description and list of the mobile device against which search was ordered; e) a description and list of the performed activities; f) a description and list of the data discovered on the occasion of the search; g) signature or stamp of the person having conducted the search; h) signature of the persons present during the search.

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

Answer*:* If the legal requirements are met, the mobile device can be searched without any restrictions. Please note that the search is not performed directly over the mobile device. The search is performed over a copy of the mobile device system. Thus, according to the provision of article 168 para. 9 of CPC, in order to ensure the integrity of the informatics data stored on the seized objects (i.e. mobile device), the prosecutor is obliged to order the making of copies.

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?*

Answer: As a general rule, the provision of article 156 of CPC, regulates that searches are conducted by observing human dignity and without being a disproportionate interference in a person's private life. Searching a mobile device should be realised based on this principle. The CPC does not limit the search. Certainly, the search is limited solely to the mobile device described in the search warrant and for those facts related to the investigate crime. However, if, on the occasion of the search it is found that the sought data is stored in a different mobile device, and is accessible from the initial mobile device, the prosecutor shall immediately order the preservation and copying of the identified data and shall request to supplement the warrant on an emergency basis.

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

Answer*:* No, the consent is not needed and does not represent a relevant element.

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

Answer: No, the owner/person cannot be forced to unlock the device.

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

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

Answer*:* As per the provisions of article 168 para. (11) of CPC, the search of the mobile device is conducted in the presence of the suspect or the defendant. Also, a person subject to search shall be allowed to be assisted or represented by a trustworthy person. If the person subject to search is in custody or arrested, the criminal bodies shall bring him/her to assist to the search. If they cannot be brought, the search of the mobile device shall take place in the presence of a representative or a community witness.

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

Answer: Yes, the search of a mobile device can be performed by means of adequate technical devices and procedures, as per the provision of article 168 para. (1) of CPC.

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

Answer: No, irrespective of the person's quality, the search procedures should be followed.

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.*

Answer: Similar to the answer from question no. 13, the criminal investigation bodies are obliged to request an EIO. The criminal investigation bodies are no allowed to perform criminal investigations which are out of their jurisdiction. The infringement of this rule would lead to the nullity of the documents and the inadmissibility of the evidence.

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?*

Answer: In such case, the search of the data should not be approved until the location of the server or the identity of the service provider are not known. The search warrant should contain such information.

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

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?*

Answer: If the search warrant contains sufficient information regarding the data from the Cloud it such access is legal. If the data is stored in Romania, the criminal investigation bodies are obliged to follow the procedure prescribed by article 168 para. 8 of CPC. Thus, in the event that, on the occasion of a search of a mobile device, it is found that the sought data is stored in cloud, and is accessible from the initial searched mobile device, the prosecutor shall immediately order the preservation and copying of the identified computer data and shall request the Judge of rights and liberties to supplement the warrant on an emergency basis.

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?*

Answer: The criminal investigation bodies, with the prior authorization of the Judge of rights and liberties, may request traffic and location data generated or processed by providers of public electronic communications networks or providers of electronic communication services intended for the public. The judge of rights and liberties will authorize this request only if the following conditions are met:

a) there is a reasonable suspicion regarding the commission of an offence like those mentioned on question 14 or an offence of unfair competition, getaway, forgery, offences relating to non-compliance with the regime of weapons, ammunition, nuclear materials, explosives and restricted explosive precursors, an offence of non-compliance with the provisions on entry into the country waste and residues, an offence concerning the organization and exploitation of gambling or an offence concerning the legal regime of drug precursors, and offences relating to operations with products liable to have psychoactive effects similar to those caused by narcotic or psychotropic substances and products;
b) there are reasonable grounds for believing that the requested data constitute evidence;

c) the evidence could not be obtained otherwise or obtaining them would involve particular difficulties which would jeopardize the investigation or there is a danger to the safety of persons or to valuable goods;

d) the measure is proportional to the restriction of fundamental rights and freedoms, given the particularities of the case, the importance of the information or evidence to be obtained or the gravity of the crime.

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

Answer: The search of a mobile device can be performed irrespective of the type of the crime involved in the case. There are no such limitations.

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.*

Answer: According to the article 102 of CPC, evidence obtained unlawfully may not be used in criminal proceedings. Also, please note that the nullity of the document which ordered the search of the mobile device, triggers the exclusion of the obtained evidence. In addition, derived pieces of evidence are excluded if these were obtained directly from evidence obtained unlawfully and could not be obtained in another way.

However, we outline that not any violation of the legal provisions excludes the evidence, but only those that represent a substantial and significant violation of the CPC provisions or of the special legislation governing the administration of evidence, if by this violation the fairness of the criminal process is achieved by damaging the rights of the parties and which cannot be removed otherwise or which may raise serious doubt as to the reliability of the evidence.

The judge will be the one who will appreciate if the breach of the law determined the violation of the fundamental rights of the parties. In such case, even if the warrant search is not affected by nullity, the evidence should be inadmissible. Certainly, if the document which orders the search will be affected by nullity then always the evidence will be considered inadmissible.

***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.*

Answer: There is no official protocol regarding this aspect. At the level of the Romanian Public Ministry (hereinafter "***RPM***") there is an undergoing project which aims to introduce, for the first time, at the level of certain investigation bodies (i.e. Prosecutor's Office attached to the High Court of Cassation and Justice, The National Anticorruption Directorate and The Directorate for Investigation of Organized Crime and Terrorism) an unitary working methodology regarding the computer search (i.e. which includes search of a mobile device) or the technical-scientific finding on some computer data of interest for criminal prosecution. Also, through this project the RPM will purchase technical equipment (hardware) and licensed applications (software) for carrying out computer searches and a specialized professional training will be provided for the target group of the project, composed of IT specialists. The project is estimated to be finalized at the end of this year. More details regarding the project can be found at the following link: http://www.sipoca54.ro/index.php/presentation/

***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?*

Answer: At the moment there are no such available specific rules. As mentioned at question no. 31, a specific methodology should be released by the end of 2020. We have no information if this methodology will include AI technology or not.

***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?*

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

Answer: The main issue is related to the fact that in such case, to ensure that the evidence obtained from the mobile device is admissible, the criminal investigation bodies are obliged to request an EIO. This aspect would lead to the delay of the investigation, and certain data could be lost or the mobile device can be destroyed. Losing the evidence is the main issue. A procedure that could speed up this process would help. The forensic examiner should always be aware of the nature of the crime and the regional legislative framework considering that the surveillance or search of the mobile device should always be performed in the presence of the prosecutor or of the police officer.

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?*

Answer: No, there is no procedure/course of action. The prosecutor will be the one who will choose if it will request an EIO or will choose to use another instrument.

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: The majority of the criminal investigation bodies request EIO.

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

Answer: There is no cooperation mechanisms or practice with the private sector.

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: Starting with January 7, 2019, Law no. 363/2018 (hereinafter "**Law no. 363/2018**") entered into force. Law no. 363/2018 transposes Directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purpose of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

Exactly as per the provisions of the Directive 2016/680, Law no. 363/2018 provides a set of rules on processing personal data to be followed during all phases of criminal trials and applicable to all authorities involved in the prevention, investigation, detection and prosecution of criminal offences, as well as in the execution of criminal penalties. Thus, the rules apply to police, prosecutors and courts.

The personal data should be processed by criminal investigation bodies according to the provisions of the Law 363/2018, as follows:

a) process the data in a lawfully, fairly and in a transparent manner;
b) collect for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures;

Regarding sensitive data, the provisions of article 10 of the Law 363/2018 establishes that processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be allowed only where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only: (a) where authorised by Union or Member State law; (b) to protect the vital interests of the data subject or of another natural person; or (c) where such processing relates to data which are manifestly made public by the data subject. Such data may not be processed for any purpose other than confirmation of identity and shall be destroyed within 3 years of collection.

We mention that if in case of search of the mobile device it is essential that the owner/user to be present during the search procedure in order to supervise the observance of the legal provisions and to raise objections, in case of their violation. Also, if the subject of the mobile device is a lawyer, the procedure must be carried out in compliance with professional secrecy.

Mobile device search is an activity that presents many difficulties, especially since this procedure involves a high degree of interference in the privacy of the user of the mobile device. The current situation of the rules specific to this activity is unfavourable, the regulated guarantees are too few and of those provided, and many can be easily circumvented.

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?*

Answer: Beside the rules presented above, there are no supplementary guidelines or rules regarding the admissibility of electronic evidence.

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.*

Answer: The admissibility criteria are the same.

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?*

Answer: The evidence obtained with the violation of the law will be excluded, irrespective of the gravity of the procedural breach. The exclusion of unlawfully or unfairly administered evidence is the procedural sanction applicable to evidence administered in violation of the principle of legality and loyalty, and where the fundamental rights and freedoms guaranteed by the European

Convention (for example, the violation of the right to silence and not to incriminate oneself, the provocation of committing crimes etc.). As mentioned above at question no. 15 and 30, the judge will have the responsibility to analyse if the procedural rule which has not been followed has the ability to affect the reliability of the evidence or the fundamental rights. Not any breach of the procedural rules would automatically lead to inadmissibility.

***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?*

Answer: If it turns out that the data is located outside of Romanians jurisdiction, the prosecutor should immediately request an EIO. Those data which were collected from our jurisdiction will be considered admissible.

***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.*

Answer: As per the provisions of article 168 para. (9) of CPC, in order to ensure the integrity of the data stored on the mobile device, the prosecutor shall order the making of copies of them. Also, if the seizure of the mobile device would seriously hinder the activity of the person holding the mobile device, the prosecutor may order the making of copies of them. Copies should be made with adequate technical devices and procedures, of nature to ensure the integrity of the information contained by these.

Starting from these rules, we observe that when performing a mobile device search, the criminal investigation bodies should be very cautious not to alter the data. However, if the data is intentionally altered the evidence should be considered inadmissible, bearing in mind that it was obtained disloyal. If the data was altered unintentionally, and that alteration did not violate

fundamental rights and freedoms of the person (the right to defence, the right to a fair trial etc.) and the data is still reliable, it should be considered that the evidence is admissible.

***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.*

Answer: At the moment, there are no specific rules available regarding the used technology whose non-compliance would lead to inadmissibility. As previously mentioned it is expected that by the end of this year such rules/guidelines to be made available by the RPM.

***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: No relevant case-law were identified.

***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.*

Answer: There is no official established and recognized standardization of the process of collection. The RMP is in the process of elaborating such rules.

However, based on our experience in the processes of collection, the person designated to collect de data takes into consideration the following best practice manuals and guidelines: AES 27-1996 (s2012): AES recommended practice for forensic purposes — Managing recorded audio materials intended for examination issued by Audio Engineering Society, Best Practice Manuals and Guidelines issued by the European Network of Forensic Science Institute (https://enfsi.eu/documents/best-practice-manuals/). Not following the rules/procedure of such best practice manuals and guidelines will not lead to the inadmissibility of the evidence, all these documents are consultative.

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

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?*

Answer: If the procedure is followed, failure to comply with data protection law will lead to the application of administrative fines as per the provisions of article 64 of Law 363/2018 and not to the inadmissibility of the evidence.

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.*

Answer: Yes, in different cases, the court founded that the records are not authentic, and have held that: "the defendants recognize their voices on tape, the court shall not consider the evidence relevant, consisting of an audio recording which is not authentic, as long as a such a registration does not meet the following requirements: to be performed simultaneously with acoustic events contained on this and not be a copy, not to contain any interventions (deletions, insertions, intercalations of words, phrases or other counterfeit), to have been performed with technical equipment presented by those who showed the record".

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

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?*

Answer: At the moment there are no general rules or guidelines. The mobile forensic evidence does not have a certain probative value, respectively is not considered more important than other evidence (i.e. whitens, documents etc.). The CPC does not provide the obligation that such evidence must be examined by an expert witness.

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: No relevant case-law were identified.

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.*

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

Answer: At the moment there is no official recognized standardization.

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: No relevant case-law were identified.

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

51. **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?*

Answer: No rules/guidance or case-law were identified.

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

Answer: The law does not requires to be trained.

53. **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?*

Answer: If the mobile device is not seized, the electronic surveillance may be ordered for a term of 30 days. In this time of period the criminal investigation bodies should extract the evidence from the mobile device. If the mobile device is seized, the search of the mobile device must be realised in the period mentioned in the warrant. In this case, the law does not impose a limitation period, the judge will be the one who will decide.

54. **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.)?*

Answer: During the criminal proceedings, the participants have the following rights:

a) The defendant:

- not to give any statements during criminal proceedings, and their attention shall be drawn to the fact that their refusal to make any statements shall not cause them to

suffer any unfavourable consequences, and that any statement they do make may be used as evidence against them;

- to be informed of the act for which they are under investigation and the charges against them;
- to study the case file, under the provisions of law;
- to choose a lawyer and, if they cannot afford one, in cases of mandatory legal assistance the right to have a court-appointed lawyer;
- to propose the administration of certain evidence under the terms set by law, to raise objections and to argue in court;
- to file any other applications related to the settlement of the criminal and civil part of the case;
- to have an interpreter free of charge, when they cannot understand, cannot express themselves properly or cannot communicate in the Romanian language;
- to use a mediator, in cases permitted by law;
- to be informed of their rights;
- other rights set by law

b) The victim&Civil party:

- to be informed of its rights;
- to propose production of evidence by the judicial bodies, to raise objections and to make submissions;
- to file any other applications related to the settlement of the criminal part of the case;
- to be informed, within a reasonable term, on the status of the criminal investigation, upon explicit request, provided that they indicate an address on the territory of Romania, an e-mail address or an electronic messaging address, to which such information can be communicated;
- to study the case file, under the law;
- to be heard;

- to ask questions of the defendant, witnesses and experts;
- to receive an interpreter, free of charge, when they cannot understand, cannot express themselves properly or cannot communicate in the Romanian language;
- to be assisted or represented by a counsel;
- to use a mediator, in cases permitted by law;
- other rights set by law.

c) The witness:

- To avoid self-incrimination;
- To be assisted or represented by a lawyer;
- Not to give any statement if such statement would lead to his incrimination;

Regarding the prosecutor or the court, it is not adequate to say that they have "*rights*" but rather "*duties*" or "r*esponsibilities*".

d) The prosecutor:

- to supervise or conduct the criminal investigation;
- to notify the Judge for Rights and Liberties and the court;
- to initiate and use criminal action;
- to initiate and use civil action, in situations established by law:
- to sign guilty plea agreements, under the law;
- to file and use challenges and avenues of appeal set by the law against court decisions;
- to fulfil any other responsibilities set by law;

e) The court:

- The court shall adjudicate the case on trial, safeguarding the rights of the parties to trial and ensuring the submission of evidence to completely clarify the circumstances of the case in order to find out the truth, fully observing the law.

5.1 The Prosecution

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

Answer: Beside those rules mentioned above in this document, there are no requirements or guidance provided to the prosecution.

5.2 The Court

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

Answer: If the judge or the other part of the criminal trial raises doubts regarding the legality of the used methods, it could be request that such aspect to be analysed by an expert aleatory nominated by the court. Such expert should draft an expertise report where it will examine if the data was altered or not. Currently, the control of the data's reliability is for the National Institute of Forensics Expertise, acting under the authority of the Ministry of Justice and whose experts have the quality of civil servants, being completely independent to the criminal investigation bodies who collected the data. Starting with 2001, the National Institute of Forensics Expertise is affiliated at the European Network of Forensic Science Institutes.

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

Answer: The evidence do not have a value pre-established by law and are subject to the free assessment of the court, based on the assessment of all pieces of evidence produced in a case. In making a decision the existence of an offence and on a defendant's guilt, the court decides, on a justified basis, on the basis of all the assessed pieces of evidence. Conviction is ordered only when the court is convinced that the charge was proven beyond any reasonable doubt. Therefore, the evidence obtained via mobile forensics will not be considered as the "*queen of the evidence*".

5.3 The defendant and defender

58. **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 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.*

Answer: There are no rules or standards regulating such right. If the defendant has certain objections regarding the procedure, has the right to request the proof with expertise in order to verify if the data were correctly collected.

5.4 Witnesses

59. **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.*

Answer: If there is a reasonable suspicion that the life, physical integrity, freedom, assets or professional activity of a witness or of a member of their family could be jeopardized as a result of the data provided by them to judicial bodies or of their statements, the judicial bodies of competent jurisdiction shall grant them the status of threatened witness and shall order one or more of the following protection measures: a) surveillance and guard of the witness' residence or providing of a temporary dwelling space; b) accompanying and ensuring protection to the witness or to their family members during travels; c) protection of identity data, by issuing them a pseudonym under which the witness shall sign their statement; d) hearing of a witness without them being physically present, through audio-video transmission devices, with their voice and image distorted, when the other measures are not sufficient. The prosecutor orders the application of protection measures ex

officio or upon request by the witness, one of the parties or a main trial subject. In case of application of the protection measures mentioned above at letter c) and d) witness statements shall not include their real address or their identity data, these being recorded in a special register to which only criminal investigation bodies have access, under confidentiality terms.

Also, beside the status of "threatened witness" the CPC provides the status of vulnerable witness. Thus, the prosecutor may decide to grant the status of a vulnerable witness to the following categories of persons: a) witnesses who suffered a trauma as a result of the committed offence or of the subsequent behaviour of a suspect or defendant; b) underage witnesses. At the moment of granting the status of vulnerable witness, the prosecutor may order the following protection measures: a) accompanying and ensuring protection to the witness or to their family members during travels; b) hearing of a witness without them being physically present, through audio-video transmission devices, with their voice and image distorted, when the other measures are not sufficient.

5.5 The Victim

***60.* 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.*

Answer: Regarding the victim's rights, please observe our answer at question no. 54. During the pre-trial and the trial the victim has the right to propose the production of evidence or to raise objections and to make submissions. Concerning the use of the evidence, yes, the victims can use evidence obtained via mobile forensics, however such evidence will certainly have to be corroborated with other evidences (e.g. witness, expertise, documents etc.) in order to ensure a high degree of trust.

FORMOBILE

• FROM MOBILE PHONES TO COURT •

formobile@netlaw.bg

Linkedin – Formobile-

Twitter – @Formobile2019

www.formobile-project.eu

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

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: N/A