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.

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?*

Lawyer, member of Thessaloniki Bar Association

PhD Candidate at the Department of Criminal Law and Criminology, of the Law Faculty of the Aristotle University of Thessaloniki

Answer: Indication of length of answer: one line.

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

Thessaloniki, Greece

Answer: Indication of length of answer: one line.

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)*

There is no particular definition for "mobile device" *per se* in Greek Criminal Law. Such devices would fall under the general definition of "information system", set forth in Article 13(f) of the Greek Criminal Code. An "information system" is defined as *any* device or group of interconnected or related devices, one or more of which, pursuant to a program, perform automatic processing of digital data; or digital data stored, processed, retrieved or transmitted by such device or array of devices, for the purposes of their operation, use, protection and maintenance. This definition is modelled after the definition found in articles 4(1)(b) and 4(1)(c) of directive EU 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

Answer: Indication of length of answer: couple of lines.

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?*

This is possible during a police examination. According to article 257(1) of the Greek Code of Criminal Procedure (hereinafter: CCP), the persons entitled to execute investigative measures [including police personnel in cases of urgency (*in flagrante delicto*)], are entitled to body-search suspects if it is deemed useful for the discovery of truth. During such body search (or search of premises, which may only be conducted if a member of the judiciary is also present), mobile devices may be discovered. What often follows is a grey zone, where police personnel would typically have a look into the mobile device to see if any useful discoveries can be made (e.g. phone calls to a potential accomplice). Such findings are typically incorporated into their witness testimony (under oath), after their investigation is completed. Depending on whether anything useful was found and/or the device is deemed to have been generally useful in the commission of the crime or supposedly proves the existence of "special infrastructure" for the commission of the crime, the device is then seized.

However, prior to seizure a mobile device may be not only searched for in a "physical" sense; it may also be placed under remote surveillance. See answer to question 5 for more details on this.

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

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?*

In urgent cases, there is no search order, and searches are conducted by law enforcement personnel at the crime scene or where suspects or other involved persons may be found. The CCP provides for the general conditions under which a premise or body search may take place (minimum disruption, no publicity, body search on females to be conducted only by females etc). There are no special provisions with regard to the search of the mobile device itself once it has been found, apart from those regarding the privilege of confidentiality, which also apply to remote surveillance. Article 9A of the Greek Constitution prescribes a (negative) right of citizens, to be protected from the collection of personal data, especially by electronic means. This provision works in tandem with that of article 19 of the Constitution, regarding the secrecy of communication, which shall be inviolable unless for the purpose of investigating especially serious crimes, as stipulated by law.

Article 256(4)(b) CCP also stipulates that those executing the search shall make every effort to preserve the honour, privacy and secrets of the person investigated, to the extent that the latter are not related to the crime being investigated.

Article 254(1)(d) CCP and statute No. 2225/1994 provide for the conditions required to waive the confidentiality of communication and proceed with remote surveillance. This can be done for most felonies and a few grave misdemeanors, provided that the evidence sought after is absolutely indispensable for the case at hand. Surveillance is limited to the suspects and their potential accomplices and only data relevant to the case may be gathered.

Data concerning the suspect's private life shall be omitted. The latter condition is often explicitly stated in the search order, but would still apply even if it was not explicitly stated, because such investigative measures constitute a severe breach of the right to privacy and can only be executed in a way compliant to the principle of proportionality, as stipulated in article 25(1)(c) of the Greek Constitution. Furthermore, as the search for digital data stored in a mobile device may constitute processing of personal data, it would have to respect the principles laid

out in article 4 of directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes 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; data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This provision has been transposed into national law by virtue of Statute No. 4624/2019 (article 45).

It must be noted that remote surveillance may only be conducted following authorisation by the Pre-trial chamber and, in urgent cases, following temporary authorisation by the prosecutor, which must be ratified by the pre-trial chamber within 3 days.

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

   Such intervention would not be legally possible prior to seizure of the device. In practice it would also not be possible before the item is seized and forwarded to the Hellenic Police Forensic Science or Cyber Crime Divisions, as typically there would not be proper resources for this at the scene of the crime/investigation.

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

   Only read. See notes to question 4 regarding the "grey zone" between physical discovery of the device and seizure.

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

   No, but according to article 257(2) CCP, they must be asked to surrender the device before being searched.

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

   No, this would violate the right to avoid acts of self-incrimination, which is explicitly provided for in article 104(1) CCP.

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

    Yes, and asked to surrender the item prior to being searched. See above, question 8.

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

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

A search can be ordered by the prosecutor or the investigator in order to uncover a crime and its perpetrators and to assist in their arrest (article 253(a) CCP). In cases of urgency (in flagrante delicto), law enforcement personnel may proceed with searches without such orders, so as to uncover the crime and its perpetrators.

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

It does. With regard to the search for the physical device, normally such investigative measures are executed only against the accused. They may be executed against third persons only if there are grave suspicions that traces/evidence of the crime may still be found. With regard to lifting of confidentiality of communication, this would only be possible against the suspect or their potential accomplices.

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.*

If the authorities have no physical access to the device connected to the cloud, international cooperation instruments like the EIO or MLATs would be the only route for this, but the measure requested by these instruments would still be seizure of digital data or remote surveillance. If the authorities do have physical access to the device connected to the cloud, then they could directly proceed with seizure of digital data.

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

As far as physically searching for a mobile device is concerned, the answer is negative. However, the type of crime involved is crucial if remote surveillance is to be pursued. The latter is only possible in order to uncover most felonies and selected grave misdemeanours, as listed in article 254(1)(d) of the CCP and article 4 of statute No. 2225/1994.

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.*

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

Unless the device is eventually seized, or lawful remote surveillance takes place, information that the law enforcement authorities have obtained by gaining access to such devices prior to seizure, does not constitute separate evidence and may only indirectly become part of the case record through a police officer's witness testimony. If the device is not eventually seized, this would typically be because it was not deemed important enough for the crime being investigated. Therefore, not following the rules at this stage does not lead to inadmissibility of evidence, but serves to undermine the value of such witness testimony.

Mobile device seized

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

Yes, just like any other item that has been useful for the commission of a crime or is a product of the crime. There are, however, special provisions in the CCP as far as seizure of digital data *per se* is concerned (see next answer).

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

Search and seizure can be ordered by the prosecutor or the investigator in order to uncover a crime and its perpetrators and to assist in their arrest (article 253(a) CCP). In cases of urgency (in flagrante delicto), law enforcement personnel may proceed with searches and seizures without such orders, so as to uncover the crime and its perpetrators. The CCP does not contain special provisions with regard to the seizure of mobile devices (as physical objects) – in this regard, general provisions regarding seizure of items would apply. However, following the entry into force of the new Greek CCP (Statute No. 4620/2019), the CCP now contains special provisions with regard to the seizure of digital data stored in such devices. Article 265 CCP stipulates that such seizure may be imposed (a) on a computer system as a whole or on parts thereof and on the data stored therein, by the investigator who has physical access to them, (b) on a data storage device, by the investigator who has physical access to it, or (c) on a remote computer system or on parts thereof and on the data stored therein, or on a remote storage site

and on the data stored therein, access to which is granted through a computer system to which the investigator has physical access. In the latter case, i.e. if access to data stored in the cloud can be gained by a local computer that the investigating authorities have access to, such data are not considered to be stored remotely.

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

Yes, but under the conditions laid out in article 265(2) *et seq.* CCP. The data shall be copied to a single storage device, which becomes part of the case record. A single backup copy is also created and is to be stored securely.

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?*

Yes. Data concerning the suspect's private life and anything else irrelevant to the crime being investigated, shall not become part of the case record. The latter condition is often explicitly stated in the search and seizure order (if one exists), but would still apply even if it was not explicitly stated, because such investigative measures constitute a severe breach of the right to privacy and can only be executed in a way compliant to the principle of proportionality, as stipulated in article 25(1)(c) of the Greek Constitution. Furthermore, as the search for digital data stored in a mobile device may constitute processing of personal data, it would have to respect the principles laid out in article 4 of directive (EU) 2016/680 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes 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; data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. This provision has been transposed into national law by virtue of Statute No. 4624/2019 (article 45).

Article 256(4)(b) CCP also stipulates that those executing the search shall make every effort to preserve the honour, privacy and secrets of the person investigated, to the extent that the latter are not related to the crime being investigated.

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

If digital data is to be obtained through remote surveillance, the surveillance order (issued by the pre-trial chamber) defines the crimes that data may be collected for. Data that may point to other criminal activities, outside the scope of the crime that remote surveillance was ordered for, may only be used in exceptional circumstances. Article 254(5)(c) and (d) CCP stipulate that it may only be used for the uncovering of criminal organisations.

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

Not quite. The person is simply requested to surrender the items/data being sought after, prior to the execution of the investigative measures. However, consent of the person in possession of the device may render some of the formalities for the search provided for by the CCP redundant – note that this is not the case with regard to the fundamental requirement for a member of the judiciary to be present during a house search.

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

Negative. This would be an infringement of the right to non-self-incrimination, which is explicitly provided for in article 104(1) CCP.

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

Yes, they are entitled to know what the search is for and who has ordered it. After seizures are complete, they shall receive a copy of the search and seizure report, as provided for by article 256(3) CCP.

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

Yes, as long as the original data is not corrupted/altered. The CCP contains no specific provision, but this follows from the matrix of provisions regarding the investigation and the objective of the investigative measure. Tampering with evidence would render it inadmissible as this would violate the right of the accused to a fair trial, per article 171(1)(d) of the CCP and 6 of the ECHR.

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

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

Yes. Searches and seizures are conducted against the accused, and only exceptionally against other parties. See above, answer to question 12.

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.*

If the authorities have no physical access to the device connected to the cloud, international cooperation instruments like the EIO or MLATs would be the only route for this, but the measure requested by these instruments would still be seizure of digital data. If the authorities do have physical access to the device connected to the cloud, then they could directly proceed with seizure of digital data.

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*

Such data may only be seized if the investigating authorities have physical access to the device connected to the cloud storage space, in which case the location of the server/identity of the service provider will not matter, as the data is considered to be stored locally, by virtue of article 265(1)(d) CCP. If no such device is found, it will be impossible to seize such data, as authorities will not have enough information to submit an EIO/MLAT request to the proper state.

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?*

This would not be possible through search and seizure, but only through the procedure for lifting confidentiality of communication, provided for in articles 254 CCP and 4 and 5 of Statute No. 2225/1994.

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?*

According to article 5 of Statute No. 3783/2009, digital subscriber data are to be retained by service providers for a period of three years after said subscription expires, whereas various types of e-data, including traffic data and location data, are retained for a period of one year

after each communication (article 5 of Statute No. 3917/2011, transposing article 5 of directive 2006/24/EC). According to three opinions rendered by the Supreme Court's Prosecution Office (no. 9/2009, 12/2009 and 9/2011), no lifting of confidentiality is required for the "external data" of communications (traffic and location data), which may be sought after by judicial or prosecutorial authorities, as long as the principle of proportionality is observed. Content data however may only be sought after through the procedure for lifting confidentiality of communications as stipulated in Statute No. 2225/1994.

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

As far as physically seizing a mobile device and its digital data is concerned, the answer is negative. However, the type of crime involved is crucial if remote surveillance is to be pursued. The latter is only possible in order to uncover most felonies and selected grave misdemeanours, as listed in article 254(1)(d) of the CCP and article 4 of statute No. 2225/1994.

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.*

In Greek Criminal Procedure, not all violations of procedural rules lead to the invalidity of an investigative measure/inadmissibility of evidence. Such invalidity must be specifically prescribed by law, or the violation of the rule must constitute a violation of the defence rights afforded to the accused (articles 170-172 CCP). It is to be noted that as the collection of evidence is typically part of the pre-trial phase, relevant procedural invalidities must be brought up by the parties prior to the referral of the case to the trial chamber, else such breaches are considered "cured" (article 174 CCP) and the defendant's only possibility would be to request that such evidence not be taken into account by the trial chamber, in case it was collected by virtue of a criminal act [article 177(2) CCP).

For example, there is no inadmissibility if the authorities conducted a house search with undue publicity. If the authorities seized digital data but failed to properly compose the seizure report required by article 265(3) CCP, this procedural breach would have to be brought up by the accused in the pre-trial phase, else it may be considered "cured" by virtue of article 174 CCP.

On the contrary, evidence that is derived from lifting of confidentiality for a crime not in the list of article 4 of Statute No. 2225/1994, would be inadmissible. The same would be the case for digital data whose content was severely altered during the process of extraction from a seized mobile device. See also the answer to question 40.

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.*

The CCP contains no specific provisions. In practice such difficulties and the steps taken to overcome them are documented summarily by those conducting the examination/data acquisition. Typically, these actions would be committed by the expert witness(es).

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

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

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?*

Negative.

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

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 primary issues are those of jurisdiction, selection of the proper international judicial cooperation instrument, cross-boundary execution of the requested investigative measures, and surrender of the evidence collected. The question of jurisdiction is usually solved according to the rules set forth in articles 5 *et seq.* of the Greek Criminal Code. Typically, if the perpetrator is a Greek citizen and/or has acted even partially on Greek soil, the question of jurisdiction is solved in favour of the Greek courts.

If there is a matter of jurisdiction between more EU member states, the problem may be solved by referral of the case to Eurojust and in light of Framework Decision 2009/948/JHA on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings, as well as various other instruments regarding particular crime types.

A difficult legal issue that has arisen is whether, once the investigative measures have been executed by the Greek authorities in the framework of an international judicial assistance request, the defendant may request that the Greek authorities refrain from submitting the outcome/results of the investigation to the requesting state, due to procedural breaches. The issue was dealt with by a decision of the pre-trial chamber of the Court of Appeals of Athens

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

(no. 16/2016), which concluded that such a motion is legally sound, even though in the particular case it was dismissed on substantive grounds.

Typically, these are legal matters of concern for the prosecutorial and judicial authorities and not for the forensic examiner.

Answer: Indication of length of answer: couple of paragraphs

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?*

There is no specific rule, but within the EU, it has become standard practice for the EIO to be preferred, as it is a more standardised tool. MLATs have been associated with unnecessary delays and lack of uniformity.

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

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?*

Presuming the question is about the EIO directive, see answer to the immediately preceding question. The EIO is the instrument of preference.

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

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

Negative.

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

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

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.

Directive 2016/680 has been transposed into national law by virtue of articles 43 *et seq.* of Statute No. 4624/2019. Relevant provisions are, for the most part, a copy of the official Greek translation of the directive. Article 59 of this Statute points to the provisions of the CCP with regard to when and how the rights of the data subject (right of access/erasure etc) are to be exercised, thereby utilising the discretion given to member states by virtue of article 18 of the directive. The CCP itself does not contain any direct references to Statute No. 4624/2019 or its predecessor (No. 2472/1997), but contains an array of provisions aimed at safeguarding the personal data and the privacy of the accused. For example, according to article 241 CCP, the criminal investigation is conducted in writing and without any publicity. With regard to seized digital data, it is explicitly stipulated that these may be accessed only by judges, prosecutors, investigators and judicial secretaries involved in the particular case [article 265(5) CCP].

With regard to irrelevant/too private information, please see answers to questions 5, 19 and 60.

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

Please see also answers to questions 23 and 42 with regard to safeguards against tampering/falsification of seized digital data.

All information relevant to the crime being investigated may be copied and retained for as long as is necessary. This would be, at the very least, until a final and irrevocable decision is rendered on the case. At that point, the court also decides finally on what is to be done with original items and data seized. Data contained in the text of the decision is retained *ad infinitum*; the detailed case record, which according to article 265(4) CCP may contain a single copy of seized digital data, may be erased following a decision by a Committee according to Royal Decree No. 120/1966, which rules on the destruction of archives once they are no longer useful. Typically, this does not happen until at least 10 years have passed after the decision was rendered final and irrevocable for misdemeanours, and about 15 years for felonies, except for cases with great historical value or those that are still needed for a particular reason. See also answer to question 54.

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

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

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?*

Negative. See above, in particular the answers to questions 19, 21 and 30.

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

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.*

The criteria are the same for all types of evidence; namely whether the evidence was collected according to the provisions of the CCP (particularly, these of articles 253 *et seq.* CCP regarding searches and 265 CCP regarding seizure of digital data) and in a manner that does not violate the defense rights; the latter would render the process invalid per article 171(1)(d) CCP.

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

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?*

It would depend on the type of procedural breach. Some procedural breaches carry no penalty; others are only important if the person concerned chose to bring the issue up, whereas other breaches would render the process invalid regardless. For example, if digital data was obtained through a criminal act (say, through theft of the mobile device), such evidence shall be declared inadmissible at any stage [article 177(2) CCP]. The same goes if other serious formalities are not followed (for example, if no member of the judiciary is present during a house search – this is a constitutional prerequisite, per article 9 of the Constitution). Recently though, the legislative branch has made a regrettable effort to reduce or nullify the effect of grave breaches on the admissibility of evidence, particularly in the cases of felonies in the field of economic crime/corruption of state officials (article 14 of Statute No. 4637/2019).

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

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

***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?*

This is a matter of jurisdiction rather than of admissibility of evidence. In any event, the location of the cloud data is irrelevant if the crime was committed in Greece and authorities have managed to gain physical access to the device that linked to such data, or to said data via lifting of confidentiality following an EIO or MLAT assistance request. Jurisdiction of Greek criminal courts is based primarily on where the crime was committed (article 5 of the Criminal Code); if the perpetrator has physically acted on Greek soil, as would be the case if they used a computer to manipulate data in the cloud from their home in Athens, whether the cloud data was stored in a server in Taiwan may become irrelevant.

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

***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.*

See answer to question 31. It must be noted that the CCP does not contain any explicit provisions on this matter, but does stipulate that digital data must be seized (through seizure of the storage device or extraction of a copy thereof) and then verified. Verification means that the data can be accessed again and authenticated as genuine and intact [article 265(1)(c) CCP]. It could be argued, therefore, that if the data is altered in a way that such authentication is no longer possible, then falsification of evidence has taken place. In that case the defendant may file a motion for the declaration of such evidence as inadmissible, because such falsification would constitute a violation of his/her defense rights [article 171(1)(d) CCP]. There is no case

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

law of this type that I am aware of, but a pre-trial chamber dismissing such a motion and holding that the alteration of the evidence during the extraction process has not affected its actual content that would have been crucial for determining the facts of the case, is not beyond the realm of imagination.

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

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.*

See above on article 265 CCP regarding seizure of digital data without damaging their integrity. There are no specific rules on the technical methodology for extracting such data (e.g. on how to bypass security measures etc). However, if this extraction becomes the subject of expert testimony, the expert witnesses (if more than one) must be in agreement about the methods used and their conclusions (article 197 CCP).

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

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*

Negative.

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.*

See below, answer to question 50 which is identical.

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

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?*

There can be no criminal procedure without some form of processing of personal data. The CCP does not stipulate a procedural invalidity in case of data protection law or privacy law breaches. Therefore, one would have to check whether some particular formalities that are a necessary for the validity of an investigative measure, are intended to safeguard personal data/privacy, or whether a breach thereof would fall into the generic category of "violation of defence rights" prescribed in article 171(1)(d) CCP.

The answer would have to take into account the aspect of data protection law/privacy rules that has been violated. Violations such as undue publicity of an investigative measure (e.g. search&seizure) or unauthorised "leaks" of seized digital data will not render that act invalid and the evidence thereby produced will not be declared inadmissible. On the other hand, a premise search and seizure of items found therein without the presence of a member of the judiciary is a major infringement of privacy that renders these investigative acts invalid and any relevant evidence inadmissible, according to article 9(1) of the Greek Constitution and article 253 CCP.

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

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.*

Typically, it is not the admissibility of such evidence that is contested, but its quality and whether it supports the charges against the defendant. See below, answer to question 51.

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

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: Indication of length of answer: couple of paragraphs.

No type of evidence is assigned a particular probative value in Greek Criminal Procedure. Judges consider all types of evidence freely and render their verdict according to the dictates of their conscience [article 177(1) CCP]. There are no specific rules on how mobile evidence is to be interpreted, but there are rules about how it is to be collected (see answers to an array of previous questions, in particular questions 17 and 19). Article 265(2-6) CCP, *inter alia*, sets forth the conditions under which such data may be seized and stored until trial, safe from tampering or accidental corruption/loss. If these conditions are followed, then the evidence is reliable in a technical sense. Whether it is sufficient for a guilty verdict is a substantive matter.

It is not obligatory by law for such evidence to be examined by an expert witness, even though it is quite often the case, as in-depth analysis of such evidence typically requires expertise in a particular scientific field (article 183 CCP). According to this article, an expert witness may be ordered to submit his/her opinion by the investigator or the Court, if expertise in a particular

science, art or technical field is necessary in order to properly evaluate the facts of the case. An expert witness can be appointed *proprio motu* or at the request of the parties of the criminal process. With regard to digital data and mobile devices, the expert witness would typically have expertise in the field of informatics and is selected from the list of expert witness of such specialty, which is compiled every September.

There are specific rules regarding persons who may not act in the capacity of an expert witness due to having a vested interest in the outcome of the case or to lacking the ability to impartially examine the issues at hand, primarily due to age or mental health issues (article188 CP).

Mobile forensic operations are generally conducted by the Hellenic Police Forensic Science or Cyber Crime Divisions, which are headquartered in Athens and have a subdivision in Thessaloniki. This means that there are some standard practices in place for mobile forensic operations and therefore evidence is presented in a relatively consistent manner.

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.*

There is a number of cases where evidence extracted from mobile devices has been evaluated by Greek Courts. Most often this has happened in cases of child pornography data stored on mobile phones. Supreme Court (Areios Pagos) cases No. 319/2017 and 1557/12 dealt with such issues. The evidence was considered to be reliable and was not contested.

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.*

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

With regard to the first part of the question, please see previous answers citing article 265 of the Greek CCP plus answer to question 48 regarding expert testimony. The second part of the question is not easy to comprehend because the 'impact of the evidence and its acceptance by the courts' is a reflection of its quality and of its collection according to the process stipulated in articles 253 *et seq.* and in particular 265 of the CCP. The quality of evidence has no impact on its validity, but only on its merits, i.e. on how it is evaluated by the judicial and prosecutorial authorities (as sufficient or insufficient). If the evidence is completely irrelevant to the case at hand, then it is a possibility that it could be ruled out as completely inadmissible.

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

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.*

Not that I am aware of. Typically, evidence collected through IT forensics is considered completely reliable.

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?*

The main issue is that evidence must be retained in its original form. The defendant is entitled to call witnesses, to appoint a technical delegate who will assist the expert witness (articles 204 *et. seq.* CCP), to file motions for procedural invalidities (articles 174-176 CCP), to request that evidence be considered inadmissible due a breach of article 177(2) CCP if such evidence was the product of a criminal act, to be tried within reasonable time in a public trial conducted by impartial and independent judges. Please see also answers to questions 23 and 42.

There is generic case law about all of these issues but none pertinent to breaches of the right to a fair trial owing to misconduct of the authorities regarding digital data/mobile forensics.

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

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?*

The only requirement is for expert witnesses to have expertise in the relevant field, which typically is the field of informatics (articles 185-186 CCP). It is legally acceptable for all other parties not to have any special training in this field.

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

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?*

If the data is physically stored in a mobile device that has been seized by authorities, there is no hard limit apart from that imposed by the statute of limitations for the crime at hand and the right of the defendant to be tried within reasonable time, as provided for by article 6 of the

ECHR. Given that such extraction of evidence typically takes place in the pre-trial stage, authorities must take into account the total amount of time that the case would require in order to be heard in court. Furthermore, if the extraction of evidence requires the lifting of confidentiality and the submission of information from service providers, these actions must take place within the limits prescribed in the answer to question 28, else the data would no longer be available.

Stricter time limits apply if such investigative measures are requested through an EIO, pursuant to article 12 of directive 2014/41/EU, which has been transposed into national law by virtue of Statute No. 4489/2017 (article 14). In that case the investigative measure shall be executed within 90 days following the decision on the recognition or execution of the EIO, unless there are grounds for postponement per article 15 of the EIO directive.

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

***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.)?*

Answer: Indication of length of answer: couple of paragraphs per different participant.

The authority to press charges is vested in the prosecution office [article 27(1) CCP]. The prosecutor is in charge of the investigation prior to trial and may order that certain investigative measures are executed (articles 30 and 32 CCP). At trial and pre-trial chambers, the prosecutor is not a party of the trial but a member of the bench, and shall objectively evaluate the facts of the case before submitting his/her opinion on the motions of the defendant and the civil party, and on the potential verdict and punishment. No decision of a Greek Court or pre-trial chamber and no order of a Greek investigator is valid, unless the prosecutor has previously delivered his/her opinion on the matter at hand [articles 30(2) and 178(2) CCP].

A case is referred to the trial chamber either by the pre-trial chamber or by the prosecutor, depending on the type of crime involved and the relevant provisions of the CCP (articles 43, 245, 308-309).

The Court (pre-trial and trial chambers) has the final say on all legal and factual issues of the case. Before reaching a verdict, the Court has the power to examine all types of evidence, to decide on their admissibility, and to request that more evidence be brought before it.

The defendant's rights are laid out extensively in articles 89-106 and 244 CCP. *Inter alia*, the defendant has access to the case record, the right to remain silent, to avoid acts of self-incrimination, to be represented by counsel, to be informed of the charges or suspicions against him/her in a language that he/she comprehends, to have the process translated to him, to communicate with at least one person of their choice, and, importantly, to ask for investigative measures to be carried out in his defence.

The victim has a dual role; typically, as a witness but also as a 'civil party', pursuing a guilty verdict. In the latter capacity the victim may be represented by counsel, file motions before the prosecutor, pre-trial chamber or court, regarding procedural issues (e.g. the inadmissibility of evidence), and may submit evidence for the case record (article 107 CCP). The civil party also has full access to the case record.

Witnesses have the least rights in Greek criminal procedure. Witnesses shall appear before the judicial authorities whenever summoned, and testify what they know about the facts of the case. They cannot be represented in Court nor can they submit requests before the authorities. Under certain circumstances, they may refuse testimony (e.g. if such testimony would violate their professional secrecy – article 212 CCP). Witnesses also are not to be punished for perjury, if they have lied before the authorities in order to shield a relative against criminal liability [article 224 (3) of the Criminal Code].

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?*

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

The Supreme Prosecution Office has issued opinions with regard to whether lifting of confidentiality is required (see answer to question 28), and directives with regard to how and when cases are to be referred to the Cyber Crime Division of the Hellenic Police for forensic examination (directive 2/22.05.2019).

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

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. During the pre-trial phase, the defendant may file a motion before the pre-trial chamber, asking the latter declare evidence inadmissible due to procedural breaches (articles 174-176 CCP). Such breaches may have taken place in the process of searching and seizing the mobile device/digital data (articles 253 *et seq.*, 265 CCP, as well as articles 4-5 of Statute No. 2225/1994 if lifting of confidentiality is involved), or the process of acquiring expert witness testimony on the matter (articles 183-202 CCP).

The actual probative value of the evidence is a matter of (substantive) judgment.

As article 265 CCP is a new provision, sadly there is no case law with regard to procedural breaches in the process of seizing digital data in particular. There is ample case law with regard to breaches of Statute No. 2225/1994 on the lifting of confidentiality, or with regard to breaches of the procedure for the delivery of expert witness testimony, which can be presented if deemed relevant.

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

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

Please see answer to question 48. On a substantive level, evidence originating from information systems is generally considered reliable. The primary issues, particularly in child pornography cases, is that of causality and knowledge – whether the fact that such data was stored in a storage device was a result of their actions or of an automated process (cache memory), whether the defendant possessed the device and knew that such data existed, and whether deleted (but recoverable) files can be evidence of previous criminal activity. Typically, courts answer these questions in the affirmative if the data is found on a device that the defendant actually possessed. See Supreme Court Decisions No. 768/2019, 1519/2017, 1517/2016.

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

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 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.*

The defendant has access to the case record, per article 100 CCP, whenever they are called to account, at regular intervals during the main investigation process and at all times after their case has been referred to the trial chamber [articles 100 and 321(6) CCP]. Article 265(3) CCP stipulates that seizure of digital data per article 265(1) and (2) CCP is documented in a report, which details the manner in which the data was seized/copied/verified/authenticated. The defendant and his defender have access to the report.

It must be noted that prior to Statute No. 4620/2019, i.e. the new Greek Code of Criminal Procedure which entered into force on 1 July 2019 , there was no special provision for seizure of digital data, and the whole matter was dealt with by virtue of the common provisions on seizure of items. Article 265 CCP is a new provision and therefore, relevant case law is virtually non-existent.

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

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

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.*

The pre-trial phase is not public. Typically, each witness is examined separately [article 225(1) CCP]. They shall only be asked regarding their knowledge or lack thereof of the facts of the crime being investigated (articles 223 and 239 CCP). They have no obligation to testify regarding matters that may establish criminal responsibility of their own or their relatives [articles 223(4) CCP and 224(3) of the Criminal Code]. They should not be asked about irrelevant matters and should be interrupted if they venture to such on their own [article 223(2) CCP].

There are no legal requirements in the CCP for witnesses regarding their capability to testify in terms of mobile forensics. However, article 203 CCP provides for a special category of witnesses, who may be summoned in lieu of expert witnesses. These are witnesses with a particular scientific expertise who may testify about a situation that no longer exists and thus cannot be the subject matter of an expert testimony. It is imaginable that such testimony would be sought after in case of corrupt or lost digital data. Unfortunately, I am not aware of any relevant case law with regard to mobile devices/forensics.

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

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

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.*

See answer to question 55. The pre-trial phase is not public and therefore, the victim's privacy is not in danger provided that the data of the case is processed according to Statute No. 4624/2019 by the authorities. The trial phase is public unless publicity may be detrimental to the private or family life of the parties, particularly in the case of sex crimes or of crimes against minors [article 330(1) CCP]. The victim may freely cite/utilise any evidence that has been lawfully collected.

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

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