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?*

Answer: *Sorainen*

Mihkel Miidla, partner

Kirsi Koistinen, associate

Norman Aas, counsel

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

Answer: Estonia

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: The term "Mobile device", is not defined under Estonian law.

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:

Under Estonian law mobile devices can be read and searched covertly as part of the surveillance activities described in Chapter 3[1] of the Code of Criminal Procedure[1] (CCP) or by a Security Authority in accordance with section 27 of the Security Authorities Act[2].

According to section 126[2] of the CCP, the Police and Border Guard Board, the Security Police Board, the Tax and Customs Board, the Military Police, the Prisons Department of the Ministry of Justice and prisons may conduct surveillance activities on the following bases:

- a need to collect information about the preparation of a criminal offence for the purpose of detection and prevention thereof;
- the execution of an order on declaring a person a fugitive;
- a need to collect information in confiscation proceedings;
- a need to collect information in criminal proceedings about a criminal offence.

Furthermore, subsection 126[2] (2) of the CCP provides a catalogue of serious crimes for which surveillance activities may be used.

---

[1] *Code of Criminal Procedure* (Available in English at: https://www.riigiteataja.ee/en/eli/ee/530102013093/consolide/current)

[2] *Security Authorities Act* (Available in English at: https://www.riigiteataja.ee/en/eli/ee/503062020002/consolide/current)

The covert examination (a type of surveillance activity) of computers and other digital devices (incl. mobile phones) is regulated in more detail in section 126[5] of the CCP. According to that section, a covert examination of a mobile device generally requires a prosecutor's order, however, if reviewing the content requires secret access to the device or the use of special software (as is the case in most cases), a court order is required.

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?*

Answer:

According to Art. 126[5] of the CCP covert examination may be conducted under written permission (an order) from the Prosecutor's Office. Such permission may be granted for a period of 2 months and is renewable for a maximum of 1 year in total.

If reviewing the content requires secret access to the device or the use of special software (as is most cases), then a separate court order is required (subsection 126[4] (5) of the CCP).

Please note that section 126[5] of the CCP applies only to the covert examination of information which is already stored on a mobile device. Any kind of interception of active calls or internet traffic by a state authority always requires a court's permission.

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

Answer:

Yes, if covert entry into a computer system (incl. mobile phone) is necessary for conducting surveillance activities or to install and remove technical applications necessary for such surveillance (e.g. special spyware), then the Prosecutor's Office may apply for a separate permission from a preliminary investigation judge for such purpose (in accordance with subsection 126[4] (5) of the CCP.

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

Answer:

According to section 126[5] of the CCP, the information collected in the course of the surveillance activities, shall be, if necessary, video recorded, photographed or copied or recorded in another way.

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

Answer:

The consent of the owner or possessor of the device is not required to conduct covert surveillance activities in accordance with the CCP or the Security Authorities Act.

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

Answer:

Estonian law does not foresee the inclusion of the owner or the possessor of the device in the covert surveillance activities and thus does not prescribe conditions, where unlocking the device would be obligatory in relation to such activities.

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

Answer:

According to section 126^{13} of the CCP, upon expiry of the term of a permission for the conduct of surveillance activities and, when several surveillance activities are conducted that coincide at least partly in time, then upon expiry of the term of the last permission the surveillance agency shall immediately notify the person with respect to whom the surveillance activities were conducted and the persons whose private or family life was significantly violated by the surveillance activities and who were identified in the course of the proceedings. Such persons must be notified of the time and type of surveillance activities conducted with respect to him or her.

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

Answer:

According to section 126^{5} of the CCP, covert examination may be conducted under a written permission (an order) from the Prosecutor's Office. permission may be granted for a period of 2 months and is renewable in total for a maximum of 1 year. Subsection 126^{2} (2) of the CCP provides for an exact catalogue of crimes for which surveillance activities may be used.

If reviewing the content requires secret access to the device or the use of special software (as is the case in most cases), a separate court order is required (section 126^{4}(5) of the CCP).

This regulation only applies only to the covert examination of information already on a mobile phone already stored on a mobile phone. Intercepting active calls or internet traffic always requires a court's permission (subsection 126^4 (5) of the CCP).

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

Answer:

Estonian law does not differentiate between the possible roles of the possessor of the device, however it should be noted that the conditions for covert examination of mobile devices are seemingly stricter, if the mobile device belongs to the suspect or the accused person. In addition, the surveillance activities may be conducted only in respect of persons with regard to whom there is good reason to believe that he or she interacts with the suspect, communicates information to him or her, provides assistance to him or her or allows him or her to use his or her means of communication (subsection 126^2 (4)).

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:

There is no specific procedure prescribed under the CCP or the Security Authorities Act to access or read data stored in the Cloud prescribed under the CCP or the Security Authority´s Act. Nevertheless, it should be noted that the Advisory Guidelines on IT-Evidence claim that in case of public investigative measures and covert surveillance, no request for legal assistance is needed for accessing and gathering data which is stored in the Cloud on foreign states' servers. The justification behind this claim is that the action of access is performed by an Estonian body conducting proceedings in the territory of Estonia and that the data can be received without physically leaving the territory of Estonia and that Estonia has the jurisdiction to copy the data. However, as these guidelines are not hard law, nor is there relevant case law available for review then we cannot confirm, what is the procedure to access or read data in the Cloud at this time.

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

Answer:

Subsection 126[2] (2) of the CCP provides for an exact catalogue of crimes (all serious crimes, including child pornography and terrorism) for which covert examination of mobile devices and computers may be used. Ordinary, non-covert search is possible for all criminal investigations.

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:

Not following the applicable rules does not always lead to inadmissibility in court, however, the general norm is that evidence, which could not have been collected by following the applicable rules, is not admissible in court. Furthermore, according to the court practice, a deliberate and intentional breach of procedural law may also render the evidence inadmissible.[3]

Still, even stricter rules apply for covert surveillance activities and thus information obtained by surveillance activities is admissible only if the application and granting of the authorisation for the surveillance activities and the conduct of surveillance activities complies with the requirements of the law (subsection 126[1] (4) of the CCP).

Mobile device seized

Disclaimer:

By providing answers to the questions in the following sections, it is assumed that "electronic evidence" or "electronic data" refers to only digital information accessed and gathered through mobile forensics. This means that the device being examined has been confiscated by law enforcement officials and being examined by an expert designated by a law enforcement official. The following answers do not cover the admissibility of digital evidence accessed or gathered in any other way.

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

Answer:

[3] The judgment of the Criminal Chamber of the Supreme Court of 29.12.2006 No. 3-1-1-97-06, clauses 31 and 32. (Available only in Estonian at https://www.riigikohus.ee/et/lahendid?asjaNr=3-1-1-97-06).

Yes, mobile devices can be seized as an object of the crime, during covert surveillance activities or confiscated as part of a search for evidence in accordance with the CCP or by a Security Authority in the course of in accordance with section 21[1] of the Security Authorities Act.

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

Answer:

All items (incl. mobile phones) may be seized as physical evidence during an inspection under section 83 or a search under section 91 of the CCP. It is important to note that the search described in section 91 can be performed only at the request of the Prosecutor's Office, under a valid search warrant and on the basis of an order from a preliminary investigation judge or the court. A prosecutor's order is sufficient to search a suspect's premises in accordance with section 83 of the CCP. Nevertheless, ordinary or non-covert search is possible for all criminal investigations.

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

Answer:

If the mobile device has come into the possession of the investigating authority as a result of a lawful act (e.g. through search), then it may be examined and relevant information thereof copied. As a rule, the seizure of the mobile phone itself is carried out in accordance with the search rules (section 91 of the CCP) and the content thereof is examined in accordance with section 83 of the CCP. Additionally, if a mobile device has been handed over to the investigating authority on a voluntary basis, then the device will be inspected in accordance with section 83 of the CCP.

In more complex cases, an investigator may also order a separate IT-expertise of the seized device, e.g. to find hidden files. The conduct of the expertise is regulated separately by law (Division 7 of Chapter 3 of the CCP) and is performed by the respective experts.

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:

There are no specific limits to the search. However, the search warrant must specify exactly which objects are to be searched. For example, if only illegal firearms are allowed to be searched and seized, then mobile phones cannot be seized during that search. Nevertheless, as digital evidence is becoming increasingly important for solving complex crimes, the courts generally allow mobile devices to be searched and seized. Furthermore, it should be noted that evidence seized during the criminal proceedings must be immediately returned to the person, if this does not hinder the criminal proceedings and/or the copy of relevant data has been made.

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

Answer:

Consent of the owner or person in possession of the device is not relevant.

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

Answer:

The owner or person in possession of the mobile device 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?*

Answer:

The owner or person in possession of the mobile device must be informed only in case of a covert examination of a mobile device (see explanations for section 126[13] above). This is because during an ordinary or non-covert search, it can be presumed that a person will know which items were seized from him or her. In addition, as a general rule, the possessor must sign the search report. as well.

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

Answer:

Yes, the use of technical tools to bypass security measures as well as requesting PIN and PUK codes from mobile service providers, is permitted.

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

Answer:

Status of the owner or possessor of the mobile device is not directly relevant. However, the conditions for covert examination are seemingly stricter if the device does not belong to the suspect or the accused person. The surveillance activities may be conducted only in respect of a person with regard to whom there is good reason to believe that he or she interacts with the suspect, communicates information to him or her, provides assistance to him or her or allows him or her to use his or her means of communication (subsection 126^2 (4)).

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:

Generally, such inquiries are made through international legal assistance and sent for execution to the country where the company operating the cloud is located.

There are no clear rules in the law as to whether an investigative body has the right to examine and copy content from the Cloud if it can be accessed through the mobile device without the consent of the owner or possessor. Nevertheless, it should be noted that the Advisory Guidelines on IT-Evidence claim that in case of public investigative measures and covert surveillance, no request for legal assistance is needed for accessing and gathering data which is stored in the cloud on foreign states' servers. The justification behind this claim is that the action of access is performed by an Estonian body conducting proceedings in the territory of Estonia and that the data is received without physically leaving the territory of Estonia as well as that Estonia has the jurisdiction to copy such data. Still, as these guidelines are not hard law, nor is there relevant case law available for review, then we cannot confirm access to Data stored on servers located outside the jurisdiction of Estonia at this time.

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:

Please see answer above.

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:

No. It is imperative that the investigative body legally owns a person's mobile device that allows open access to the cloud content associated with that person. But even in latter case, there are no clear rules, as described above.

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:

Access to data (such as PUK and PIN codes) kept by a Service Provider can be requested by the investigative authorities under subsection 32 (2) of the CCP, however, a court order is needed if the service provider is required to disclose information protected by the confidentiality of messages.

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

Answer:

The foregoing is not dependent on the type of crime and is applicable to all criminal proceedings. Only in the case of surveillance activities, subsection 126^2 (2) of the CCP provides for an exact catalogue of crimes (all serious crimes, including child pornography and terrorism) for which surveillance activities may be used.

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:

Not following the applicable rules does not always lead to inadmissibility in court, however, the general norm is that evidence, which could not have been collected by following the applicable rules, is not

admissible in court. Furthermore, according to court practices, a deliberate and intentional breach of procedural law may render evidence inadmissible.[4]

Still, even stricter rules apply for covert surveillance activities and subsequently information obtained by activities is admissible only if the application and granting of the authorisation for the surveillance activities and the conduct of such activities complies with the requirements of the law (subsection 126[1] (4) of the CCP).

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.*

Answer:

No such strict protocol has been prescribed under Estonian law or discussed in court practices. However, the case-law has accepted the method of making a reference copy of the device (with the hash function), which can be used to compare and verify changes made at a later stage.

[4] The judgment of the Criminal Chamber of the Supreme Court of 29.12.2006 No. 3-1-1-97-06, clauses 31 and 32. (Available only in Estonian at https://www.riigikohus.ee/et/lahendid?asjaNr=3-1-1-97-06).

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:

No specific rules regulating the use of mobile forensics tools or deploying AI technology have been prescribed under Estonian law.

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 na ture of the crime and the regional laws/legislative framework?*

Answer:

The main issues in Estonia with cases involving mobile devices involved in crimes across geographical boundaries, is the lack of cooperation and information sharing between the different authorities as well as the question of jurisdiction. One of the reasons for the inadequate sharing of information and cooperation is the lack of effective and specific guidelines and procedures regarding data from mobile devices and subsequent international cooperation.

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 such procedure or course of action has been established in Estonia in relation to data from mobile devices at this time.

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:

We would kindly ask that you clarify this question.

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

Answer:

Estonian service providers have an extensive and extended history of cooperation with the Prosecutor's Office, however, no official cooperation mechanisms or practices have been published at this time.

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:

There are no special legislative acts for regulating the conduct of mobile forensics in criminal proceedings. The examination of mobile devices within the framework of criminal proceedings is subject to the general regulations on the performance of forensic examinations. These regulations are both provided in the Estonian Code of Criminal Procedure as well as in the Forensic Examination Act[5]. Neither of the aforementioned acts provide any specific regulation regarding the methods or rules for how the digital data must be analysed. The CCP mainly regulates the legal status, requirements for and the rights and obligations of the expert as well as the requirements for the final report of the examination to be submitted to the court. However, it is required under the law that the examiner must ensure that all expert enquiries are conducted thoroughly, completely and objectively and that the expert´s opinion is rendered scientifically valid (clause 98 (2) 3) of the CCP). Additionally, the method used for conducting mobile forensics must be in accordance with the applicable standards established at the time of conducting the mobile forensics.[6]

[5] Forensic Examination Act (Available in English at: https://www.riigiteataja.ee/en/eli/501042019023/consolide)

[6] Kergandberg, E., Pikamäe, P. The Code of Criminal Procedure. Comments. Tallinn: Juura 2012. Page 278, section 3.

Furthermore, the analysis of data must not violate any fundamental rights or other rights guaranteed to persons under Estonian or any other international legal act, unless there are any valid legal grounds provided to justify it. According to subsection 9 (4) of the CCP, it is permitted to interfere with the private and family life of a person only in the cases and pursuant to the procedure provided for in the CCP and in order to prevent a criminal offence, apprehend a criminal offender, ascertain the truth in a criminal matter or secure the execution of a court judgment. Whether interference with the private and family life of a person is justified or not is assessed on a case by case basis at the discretion of the courts.

As regards to the processing of personal data, the provisions established for law enforcement authorities in the Personal Data Protection Act[7] must be followed (subsection 15^2 (2) of the CCP and subsection 41 (2) of the Forensic Examination Act). In fact, when processing personal data pursuant to the CCP, a data controller may restrict the rights of a data subject arising from the Personal Data Protection Act (especially from sections 22 until section 28 of the Personal Data Protection Act), if it is required to prevent or detect an offence, to conduct proceedings with respect to an offence or to enforce a punishment, to conduct civil, administrative or any other legal proceedings, to prevent any damage to the rights and freedoms of another person or data subject, to prevent endangering of national security or to ensure maintenance of public order (subsection 15^2 (4) of the CCP).

There are no regulations in the CCP specifying how the information gathered from mobile forensics can be retained or copied and for how long. Nevertheless, if preservation of a data recording made in the course of surveillance activities and included in the criminal file is not necessary, then the person whose fundamental rights have been violated by such surveillance activities may request the destruction of the recording after the entry into force of the court judgment (subsection 126^{12} (5) of the CCP).

[7] Personal Data Protection Act (Available in English at https://www.riigiteataja.ee/en/eli/523012019001/consolide)

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: There are no general rules or guidelines on the admissibility of digital evidence applicable to mobile forensics in Estonia.

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: Yes, because Estonian law does not provide any specific rules or procedure for collecting digital evidence through mobile forensics and as a result the provisions on the admissibility of conventional evidence are applicable to digital evidence, including evidence collected through mobile forensics.

The collection of digital evidence can be performed on the basis of the CCP by means of either public investigative measures (inspection, search) or covert surveillance activities conducted secretly from a suspect. In both cases, the data must be collected and executed pursuant to the existing procedural order by a police officer or an investigative bodies' official, who is entitled to collect evidence (such as experts). Specific procedural rules for the inspection are outlined in Division 5 of Chapter 3 of the CCP, for conducting a search in division 6 of Chapter 3 of the CCP and for surveillance activities in chapter 3^1 of the CCP.

The admissibility of evidence is assessed by the court during the evaluation of the evidence and at the judges' discretion. In particular, the court will assess, whether the evidence provided has been collected by following the procedural rules of the CCP and whether any breach of procedural rules could render the evidence to be regarded as inadmissible.

There are more stricter rules for covert surveillance activities and as such the information obtained thereof is admissible only if the application and granting of the authorisation for the surveillance activities and the conduct of such activities is in compliance with the requirements of the law (subsection 126^1 (4) of the CCP). Otherwise, the evidence will not be admissible in court

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: As a general rule, it is the judges' discretion to assess the facts of a case as a whole and then to decide whether or not, in this particular case, the public interest related to establishing the facts of the case allow the evidence to be admissible. According to the practice of the Criminal Chamber of the Supreme Court, any evidence is inadmissible only if the procedural rules for gathering such evidence have been significantly violated. In doing so, it is necessary to assess the purpose of the violated regulation and whether such evidence would not have been obtained if the regulation had not been violated[8]. Additionally, according to the court practice, a deliberate and intentional breach of procedural law may also render evidence inadmissible.[9]

As regards determination of significant violation of procedural rules, it is subject to assessment of the court on the basis of the facts of each individual case and their sole discretion.

As mentioned above, stricter rules apply for covert surveillance activities. Information obtained by surveillance activities is evidence only if application for and grant of the authorisation for the surveillance activities and the conduct of such activities is in compliance with the requirements of the law (subsection 126^1 (4)).

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: The CCP does not provide any regulation for accessing and gathering of digital evidence across borders (i.e. accessing and gathering information from servers located outside the jurisdiction of Estonia).

---

[8] The judgment of the Criminal Chamber of the Supreme Court of 26.06.2009 No. 3-1-1-52-09, clause 11.1. (Available only in Estonian at https://www.riigikohus.ee/et/lahendid/?asjaNr=3-1-1-52-09)

[9] The judgment of the Criminal Chamber of the Supreme Court of 29.12.2006 No. 3-1-1-97-06, clauses 31 and 32. (Available only in Estonian at https://www.riigikohus.ee/et/lahendid?asjaNr=3-1-1-97-06)

There are also no court practices (incl. case law) available for review in lieu of the situation described in the provided question.

The CCP foresees that evidence taken in a foreign state pursuant to the legislation of such state may be used in a criminal proceeding conducted in Estonia, unless the procedural acts performed in order to obtain the evidence are in conflict with the principles of Estonian criminal procedure (subsection 65 (1) of the CCP). Subsequently, a request for legal assistance from a foreign state is usually in order. However, as this technique is not effective for collecting digital evidence, then the Advisory Guidelines on IT-Evidence (prepared by law enforcement agencies) claim that in case of public investigative measures (inspection, search) and covert surveillance, no request for legal assistance is needed for accessing and gathering data, which is stored in the Cloud on foreign states' servers. The justification behind this claim is that the action (the copying of data) is performed by an Estonian body conducting proceedings in the territory of Estonia and that the data can be received without physically leaving the territory of Estonia as well as that Estonia has the jurisdiction to copy such data.[10] The aforementioned point of view could be also applicable when digital evidence has been gathered by an expert through mobile forensic, however, we are not able to verify it as the courts have not voiced their opinion regarding the issues regarding jurisdiction yet.

Therefore, there are no certain answers to provide whether a digital evidence located outside Estonian jurisdiction during the criminal procedure through mobile forensic would be admissible or inadmissible in any case. Ultimately, this is a discretionary decision of the court.

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: The CCP does not provide any regulation as regards admissibility of evidence altered by the experts during the investigation process and there is no relevant court practices on this matter. According to subsection 286[1] (1) of the CCP, the court shall accept and organise the taking of only such evidence which

[10] E. Laurits. Criminal procedure and digital evidence in Estonia. - Digital Evidence and Electronic Signature Law Review, 13 (2016), page 118.

has relevance to the matter. Additionally, as stipulated in subsection 61 (2) of the CCP, the evidence will be evaluated in aggregate, according to the conscience of the judges.
Therefore, as deriving from the CCP, it is a discretionary decision of the court whether alteration of evidence renders it inadmissible or not.

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: No, the CCP does not provide any special regulation for the used technology, methodology in order for digital evidence to be admissible. However, according to the legal literature, experts must conduct mobile forensics by following the standards established type of forensics by taking into account the current development level of the respective discipline.[11]

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: We are not aware of any court practice regarding admissibility of the evidence produced by using mobile forensics.

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: No, the CCP does not provide any special regulations (other than what is outlined under question 38 above) for the collection, analysis, interpretation or reporting of digital evidence gathered through mobile forensics.

[11] Kergandberg, E., Pikamäe, P. The Code of Criminal Procedure. Comments. Tallinn: Juura 2012. Page 278, section 3

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: The CCP does not *expressis verbis* provide any specific grounds to declare digital evidence inadmissible due to a failure to comply with Data Protection laws, or privacy rules.

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: We are not aware of any court practice regarding evidence collected through mobile forensics, which has been questioned or rejected due to the admissibility of the evidence being questioned.

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:

There are no general rules or guidelines specifically applicable to the interpretation and presentation of evidence received from mobile forensics in Estonia, because Estonian law does not have a special procedure or specific provisions for the use of digital evidence in criminal proceedings.

Evidence received from mobile forensics does not have a certain probative value because evidence in general under Estonian law does not have predetermined weight. Furthermore, there are no special rules for assessing the reliability of evidence obtained from mobile forensics, because the competence to evaluate all evidence belongs to the court.

In addition, there is no specific requirement under law to have evidence from mobile devices examined by an expert witness, however one may be requested by the prosecution under section 105 of the CCP. The involvement of expert witnesses is not common as it does not depend on the format of the evidence and instead on its´ specific content.

There are no specific training or experience requirements for experts in Estonia, instead the CCP recommends primarily the use of state forensic institutions, however, also accepts other officially certified persons as well as other persons with the relevant knowledge as experts.

There is no centralised management of mobile forensic operations in our jurisdiction to ensure that work is compliant with standards and can be presented in court in a 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.*

Answer:

Based on the review of the available case law we did not identify any cases specifically dealing with the interpretation and presentation of evidence produced using mobile forensics. Evidence produced from mobile forensics is interpreted and presented on the same conditions as other digital evidence or evidence in general.

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.*

Answer:

There is no established or recognized standardization(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 in Estonia. Digital evidence is subject to the same requirements as evidence in general. According to section 61 of the CCP evidence cannot have predetermined weight. Therefore the validity, quality or the impact of the evidence and its acceptance by the courts cannot be predicted.

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

Answer:

The law does not stipulate conditions for the judicial control over the approaches and methods for acquiring, collecting and analysing evidence, nor have we identified case law related to the admissibility of evidence collected specifically through mobile forensics.

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?*

Answer:

There are no specific rules, guides or case law on how to respect the right to a fair trial in case of evidence extracted via mobile forensics, as the Estonian law does not have a special procedure or specific provisions for the use of digital evidence in criminal proceedings. There are no specific practices (incl. case law) specifically related to the principle of equality of arms and evidence extracted via mobile forensics either. Therefore, general rules on the right to a fair trial have to be taken into account, by respecting the principle of equality of arms.

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?*

Answer:

There is no training required by law for prosecution, expert witnesses or lawyers involved in cases with evidence originating from mobile forensics.

Judges are required to develop knowledge and skills by participating in trainings on a regular basis. However, this is a general obligation provided by the law. The law does not require participating in a training

specifically regarding cases with evidence originating from mobile forensics. If such a training exists (we don't have such relevant information) and it is part of the judge's professions skills training program approved by the official Training Council, the participation is mandatory.

However, an expert witness must prove to the court that he or she has sufficient knowledge and experience in the relevant field.

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?*

Answer:

An inspection, including the extraction of evidence from mobile device and other above mentioned activities are not limited in time by law. The investigation can be performed as long as a body conducting the proceedings deems it necessary. Still it should be noted that the general procedural time limits apply, i.e. the criminal proceedings must be conducted within a reasonable time.

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:

Estonian regulation does not separate the procedural rights inherent to the different participants in a criminal procedure regarding the use of mobile forensics. Therefore, answering to this question, we have described the general rights of different parties in criminal proceedings.

The prosecution

The Prosecutor's Office directs the pre-court proceedings and ensures the legality and efficiency thereof and represents the public prosecution in court. Additionally, Prosecutor's Office has the right to file a civil action or proof of claim in public law. The Prosecutor's Office prepares the statement of charges.

The court

The general principle is that the courts must be independent in their activities and shall administer justice in accordance with the Constitution and the laws. The court has the right to give permissions to collect certain type of evidence during pre-court proceedings and during the criminal proceedings as well. During the

criminal proceedings, court has the right to assess the facts of a case by deciding whether or not, in this particular case, the acquired evidence of this case is admissible.

The suspected/accused person

According to section 34 of the CCP, the suspect has the right to:

1) know the content of the suspicion and give or refuse to give testimony;
2) know that his or her testimony may be used in order to bring charges against him or her;
3) the assistance of an interpreter or translator and counsel;
4) confer with the counsel without the presence of other persons;
5) be interrogated and participate in confrontation, comparison of testimony to circumstances and presentation for identification in the presence of a counsel;
6) participate in the hearing of an application for an arrest warrant in court;
7) submit evidence, requests and complaints;
8) examine the minutes of procedural acts and give statements on the conditions, course, results and minutes of the procedural acts, with such statements being recorded in the minutes;
9) give consent to the application of settlement proceedings, participate in the negotiations for settlement proceedings, make proposals concerning the type and term of punishment and enter or decline to enter into an agreement concerning settlement proceedings.

In certain circumstances (specified in section 34^1 of the CCP) a suspect has the right to request access to the evidence, which is essential for specifying the content of the suspicion filed against them or for deciding whether the arrest warrant is justified.

According to section 35 of the CCP, the accused has the right to examine the criminal file through his or her counsel and participate in the judicial hearing.

The witness

A witness may request the presence of a counsel at the interrogation in the pre-court proceedings (section 67^1 of the CCP). In certain circumstances (specified in sections 71-73 of the CCP), a person has the right to refuse to give testimony as a witness. This is because under Estonian law no one may be compelled to testify against himself or herself, or against those closest to him or her (the descendants and ascendants, sisters and brothers, step or foster parents and children, spouses etc.). The right to refuse to give testimony as a witness may be relevant also in regard to professional activities (ministers of religion, counsels and notaries, health

care professionals, pharmacists etc.). A person can also refuse to give testimony concerning state secrets or classified information of foreign states.

The victim

According to section 38 of the CCP, a victim has the right to:

1) contest the refusal to commence or termination of criminal proceedings;
2) file a civil action or proof of claim in public law through an investigative body or the Prosecutor's Office;
3) give or refuse to give testimony;
4) submit evidence, requests and complaints;
5) examine the minutes of procedural acts and give statements on the conditions, course, results and minutes of the procedural acts, with such statements being recorded in the minutes;
6) examine the materials of the criminal file;
7) participate in judicial hearing;
8) give consent to the application of settlement proceedings or to refuse to give such consent, to present an opinion concerning the charges and punishment and the amount of damage set out in the charges and the civil action or the proof of claim in public law;
9) give consent to the application of temporary restraining order and request application of restraining order;
10) request that his or her questioning be conducted by a person of the same sex when it comes to sexual violence, gender violence or a criminal offence committed in close relationship.

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?*

Answer:

According to the information received from the district prosecutor's master's thesis, the Prosecutor's Office has an advisory guideline for processing digital evidence. This guide provides instructions on how to collect digital evidence during the pre-trial criminal procedure and how to handle it. The aim of this guide is to harmonise the practice of collecting digital evidence in different Prosecutor's Offices and investigative

bodies by explaining mainly the general principles. However, this guide is not available to the public and thus we have not reviewed or analysed it.

5.2 The Court

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

Answer:

The court has the right to give permission to collect certain type of evidence, for example evidence collected during surveillance activities, such as wire-tapping mobile devices. Surveillance activities may be conducted with a written permission from the Prosecutor's Office or from a preliminary investigation judge. The preliminary investigation judge decides, on the basis of a reasoned application, whether to grant or refuse permission to conduct the surveillance activities (subsection 126^4 (1) of the CCP). As stated above, a court order is also generally required for conducting a search in accordance with section 91 of the CCP.

Additionally, during the criminal proceedings, the court has the right to assess the facts of the case and decide whether or not the evidence is admissible.

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

Answer:

There are no special rules for assessing the evidence obtained via mobile forensics, therefore we do not have relevant case law to refer to at this time. As no evidence has predetermined weight in Estonia, the court shall evaluate all evidence in the aggregate according to the conscience of the judges.

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.*

Answer:

There are no such rules or standards regulating separately the defendant's and his/her defender's rights. If the mobile device is considered as an object of a criminal offence, it can be confiscated from the defendant after which, usually, a copy is made from the digital device. This is particularly relevant for the observations of hard disks of computers and servers, as the confiscation of the device can significantly hamper the day-to-day operation of their owners. However, it is not allowed to return evidence containing for example, a computer virus, malware or child pornography, etc., in which case the court decides which measures will be taken regarding the evidence (usually such kind of data is destroyed). The evidence confiscated during the criminal proceedings must be immediately returned to the defendant, if this does not hinder the criminal proceedings and/or a copy of relevant data has been made.

In a relevant court case, a hard drive of a computer, which also contained several images of child pornography, was confiscated from the defendant during criminal proceedings. The defendant was convicted and therefore the court decided to destroy the whole hard drive, instead of deleting only the relevant pictures thereof. This court judgement was appealed by the defendant, who requested that the remaining data on the hard drive (excluding the images of child pornography) needs to be copied and returned to him. The Supreme Court found that:

- where possible, the relevant data should be copied or deleted from the computer or made inaccessible to the defendant. The computer, computer system or storage medium as a whole should not be confiscated, if possible;
- the court has to consider the possibility of returning the data stored on the hard drive, which has no connection with the crime and for which the defendant was not convicted;
- in addition to the unlawful images, it has been decided to confiscate lawful materials which might be necessary for the defendant. Therefore, the court has to decide whether destroying the whole

hard drive would infringe defendant's fundamental right to property and whether such an infringement is proportionate.[12]

According to the law, the defence lawyer has the right to have access to all evidence, including seized mobile devices, at the end of the preliminary investigation, however, the defence lawyer is not entitled to physical possession of it. The defence lawyer may also not obtain information, submission of which may result in communication of information concerning the methods, tactics of a surveillance agency and the equipment used in conduct of surveillance activities (section 126[14] of the CCP).

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.*

Answer:

Considering the gravity of a criminal offence or the exceptional circumstances relating thereto, the witness can be declared anonymous in order to ensure their safety (section 67 of the CCP). In such cases, a fictious name shall be assigned to the anonymous witness and the information with sensitive information (name, personal identification code, date of birth, residence and place of employment, etc.) will be kept separately from the criminal file. During the court proceedings, the anonymous witness shall be heard by telephone and using voice distortion equipment, if necessary.

There are no specific requirements for witnesses regarding their capability to testify in terms of mobile forensics in the pre-trial and/or the trial phase. If an expert is involved to the criminal proceedings, he or she should preferably be a nationally recognized expert from a state forensics institution (an IT-expert from the Estonian Forensics Science Institute).

[12] The judgement of Criminal Chamber of the Supreme Court of 16 May 2012 No. 3-1-1-57-12. (Available only in Estonian at: https://www.riigikohus.ee/lahendid?asjaNr=3-1-1-57-12)

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.*

Answer:

Estonia has implemented the Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime. This means that the investigative body and/or the Prosecutor's Office is obligated to assess, whether any circumstances exist which give reason to believe that the victim requires special treatment and protection in the criminal proceedings. Measures for special treatment and protection for victims are specified in Article 23 of this Directive.

In summary, the victims are allowed to present any evidence they find to be useful and the investigative body as well as the Prosecutor's Office must decide, whether such evidence presented by the victim will be used in the criminal proceeding.

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:

We have nothing to add at this time.