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

IMPORTANT TO READ BEFORE ANSWERING THE QUESTIONNAIRE:

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

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

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

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

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

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

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

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

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

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

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

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

Introductory questions:

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

Answer: University of Helsinki, Professor of Criminal Law.

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

Answer: Finland.

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: Yes, albeit not explicitly. Section 3 para 25 of Act on Services of Information Society (Act 917/2014) contains the definition of 'telecommunications terminal equipment'. The definition encompasses, inter alia, smartphones, tablets and smart tv's but is formulated in a device neutral manner, which makes it possible to apply the definition to various kind of devices.

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?*

In some situations, a mobile device can be searched according to the Finnish Coercive Measures Act (Act 806/2011) without seizing it but to search relevant information from the device in order to enable the forthcoming seizure. This coercive measure is called "search of data contained in a device" (Chapter 8, Section 20 of the Coercive Measures Act). A search of a data contained in a device refers to a search that is directed at the data that is contained at the time of the search in a computer, a terminal end device or in another corresponding device or information system. A search of data contained in a device may be conducted if there is reason to suspect that an offence has been committed and the most severe punishment provided for the offence is imprisonment for at least six months, or if the matter being investigated involves circumstances connected to the imposition of a corporate fine. In addition, it may be conducted if it may be presumed that the search can lead to the discovery of a document or data to be confiscated, seized or copied under Chapter 7 of Coercive Measures Act. A search of data contained in a device may also be conducted in order to return the device to a person entitled to it, if there are grounds to suspect that it has been taken from someone by an offence.

It must be noted that search of data contained in a device is directed to data that is located in the device or accessible through the device at the time of a search. Other coercive measures,

covert coercive measures, such as telecommunications interception, may be used in relation to information accessible through mobile device in the future.

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?*

Yes, there are various important limitations. Firstly, a search of a data contained in a device may not be directed to confidential message, which in turn may be a subject of some covert coercive measures (telecommunications interception, traffic data monitoring and technical surveillance) under Chapter 10 of the Coercive Measures Act). This limitation practically means that search of a data contained in a device shall not be used in situations where provisions on covert coercive measures apply, i.e. requirements set in provisions concerning covert coercive measures shall not be bypassed by using search of a data contained in a device. Secondly, search of a data contained in a device may not be used in respect to any offence but only to an offence for which the most severe punishment provided is imprisonment for at least six months. Thirdly, it must be presumed that a search can lead to the discovery of a document or data to be confiscated, seized or copied under Chapter 7 of Coercive Measures Act. These three requirements must be fulfilled in every case.

In addition, the coercive measures act contains provisions on relevant principles that in practice set important limitations on the use of the coercive measures. Firstly, according to the Section 2, Chapter 1 (Principle of Proportionality) of the Coercive Measures Act Coercive measures may be used only when they may be deemed justifiable with consideration to the seriousness of the offence under investigation, the importance of clarifying the offence, the degree to which the use of the coercive measures infringes on the rights of the suspect in the offence or of others, and the other circumstances in the case. Secondly, Section 3 of the same Chapter contains provision on the principle of minimum intervention, according to which the use of a coercive measure may not infringe on the rights of anyone beyond what is necessary in order to achieve the purpose for which it is used and the use of a coercive measure may not cause anyone undue

loss or impediment. Lastly, Section 4 of the mentioned Chapter contain a provision on the principle of sensitivity, which states that in the use of coercive measures the arousing of undue attention shall be avoided and also otherwise conduct shall be discrete.

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

   No, at least the Finnish legislation does not explicitly allow it.

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

   Yes, but this is possible only when a separate decision on copying is issued in accordance with Chapter 7, Section 2 and 7 of Coercive Measures Act.

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

   No, albeit there is no explicit provision on the matter.

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

   Under certain circumstances yes. If the person in possession of the mobile device is not cooperative and if the legal requirements set for search of a data contained in a device are fulfilled and the measures is used in relation to suspected offence, the personal identifying characteristics (such as fingerprints) of the suspected person may be taken (Chapter 9, Section 3 of the Coercive Measures Act) and the mobile device may be unlocked with the help of these identifying characteristics.

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

    Yes.

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

    An official with the power of arrest. The definition of an official with the power of arrest is to be found on Chapter 2, Section 9 of Coercive Measures Act.

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

    The Finnish legislation does not principally restrict the search of a data contained in a device only to devices of the person suspected. This means that devices owned or possessed by a third party or a witness may in principle be searched, if the requirements set by legislation are fulfilled. In most cases, however, the search of a data contained in a device is directed to a device in possession of the person suspected of a crime.

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.*

The search of a data contained in a device may be applicable if the data in a cloud is accessible only a device that is the subject of the search. In other cases, international or regional cooperation (e.g. EIO) or Mutual Legal Assistance Treaties may be used. It has been estimated that in practice direct access to data located outside own jurisdiction may be quite common, since jurisdictional limits may be interpreted differently in different countries and authorities may not in every case even notice that the data obtained is located outside their own jurisdiction. In any case, Finnish legislation does not contain any mention on the location of data in relation to search of a data contained in a device.

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

No. Like mentioned above, search of data contained in a device is applicable in relation to all offences for which the maximum sentence provided in legislation is imprisonment for at least six months.

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.*

The Finnish Code on Judicial Procedure contains a general provision on the matter, in which the following is stated:

Chapter 17, Section 25

(1) The court may not use evidence that has been obtained through torture.

(2) The court may not, in criminal proceedings, use evidence obtained contrary to the confidentiality obligation provided in section 18. The prohibition against use applies also to evidence that was obtained from a person in proceedings other than a criminal investigation or in criminal proceedings, through the threat of coercive measures or otherwise against his or her

will, if he or she at the time was a suspect in an offence or a defendant or a criminal investigation or court proceedings were underway in respect of an offence for which he or she was charged, and if the obtaining of the evidence would have been contrary to section 18. If, however, a person in other than criminal proceedings or comparable proceedings has, in connection with fulfilling his or her statutory obligation, given a false statement or submitted a false or untruthful document or a false or forged object, this may be used as evidence in a criminal case concerning conduct in violation of his or her obligation.

(3) In other cases the court may use also evidence that has been obtained unlawfully, unless such use would endanger the conduct of a fair trial, taking into consideration the nature of the case, the seriousness of the violation of law involved in the obtaining of the evidence, the significance of the method in which the evidence was obtained in relation to its credibility, the significance of the evidence in respect of the decision in the case, and the other circumstances.

In most cases the situations meant in this question would fall under the 3rd paragraph of the referred section.

Mobile device seized

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

Yes. General provisions on confiscation (or seizure) and copying of a document (Chapter 7 of the Coercive Measures Act) are applicable also to mobile devices. (See also answer to question 17.)

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

According to the Section 1, Subsection 1, Chapter 7 of the Finnish Coercive Measures act, an object, property or document may be seized if there are grounds to suspect that 1) it may be used as evidence in criminal case, 2) it has been taken from someone in an offence or 3) it may be ordered forfeited. In subsection 2 of the mentioned provision it is explicitly stated that what

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

is stated in subsection 1, also applies to information that is contained in a technical device or in another corresponding information system or in its recording platform (data).

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

Yes. According to the Section 2, Chapter 7 of the Coercive Measures Act, seizure of a document to be used as evidence shall be replaced by copying of the said document if a copy is sufficient from the point of view of the credibility of testimony. If a document cannot be copied without undue delay due to the nature or extent of the document or documentation, the document shall be seized.

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, there are various important limitations and also exceptions to these limitations. The basic rule concerning limitations is that seizure or copying is not possible if the document contains information which according to Code on Judicial Procedure is subject to limitation from the obligation to testify. These include both situations where there is a right not to testify (these apply to, inter alia, a present or a former spouse) and obligation not to testify (these apply to, inter alia, an attorney or health care professionals). Most of these limitations do not, however, apply if, e.g., the maximum punishment for the offence under investigation is imprisonment for at least six years. This means that limitations do not apply when the suspected offence is very grave. The limitations and exceptions concerning limitations are in detail defined in Section 3, Chapter 7 of Coercive Measures Act.

See also what has been stated on the general principles guiding the use of the coercive measures under question 5.

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

No.

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

Under certain circumstances yes. See answer under question 9, which also applies to seizure.

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

Yes. According to Section 9, Chapter 7 of Coercive Measures Act the person from whose possession an object, property or document has been taken for seizure or copying shall be notified of this without delay. The person is, in other words, informed on the fact that his/her property or document has been taken to the possession of the authorities.

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

Yes. This is evident from Section 11, Chapter 7 of Coercive Measures Act in which it is stated that if needed and by the decision of the head investigator, an expert in the information system that is the object of the measure or in its recording platform may assist in the opening of the document that is in the form of data. This also includes that technical tools may be used.

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

According to Finnish legislation, seizure is possible in relation to an object, property or document and data. In the legislation there are no restrictions concerning the personal application of the relevant provision. In addition, it could be stated that the provision on the notification of the taking of possession implies broad personal application of the relevant provisions, since it is explicitly stated that the person from whose possession an object, property or document has been taken for seizure or copying shall be notified on it.

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 data is stored in the cloud and if the suspected person is known to reside outside Finnish jurisdiction, mutual legal assistance treaties and EIO are alternatives if data is located outside Finland. If data is located in Finland, relevant provisions on seizure apply.

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?*

There are no explicit provisions on the significance of the location of data in relevant Finnish legislation. It has been estimated that in practice direct access to data located outside own jurisdiction may be quite common, since jurisdictional limits may be interpreted differently in different countries and authorities may not in every case even notice that the data obtained is located outside their own jurisdiction. In any case, Finnish legislation does not contain any mention on the location of data in relation to seizure.

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?*

Section 1, subsection 2, Chapter 7 of the Coercive Measures Act is formulated in a relatively broad manner. According to it seizure (and copying) is possible when it is question of information that is contained in a technical device or in another corresponding information system or in its recording system. The definition is, however, in all situations connected to a technical device or another connecting information system. This means that the data that is stored into a recording system, must have a connection to a certain device. The purpose of the legislator has, however, been that the location of the data is not relevant and for example information in memory cards is meant to be included to the definition (see Government's Proposal 153/2006 vp).

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?*

The service providers have an obligation to store and save the relevant data for the possible purposes of authorities. This is in more detail regulated in the Act on Services of Information Society (Sections 157–159). The stored data (that may include, inter alia, data related to a telephone service or SMS service provided by the operator or data related to internet access service, but not to the contents of a message or traffic data generated through the browsing of websites) may be used only for the purposes of solving and considering charges for criminal acts referred to in Section 6, subsection 2, Chapter 10 of the Coercive Measures Act. The

provision referred regulates prerequisites for traffic data monitoring, the coercive measure which can be performed only upon a court order. In addition, according to the Section 24, Chapter 7 of the Coercive Measures Act, an official with the power of arrest may issue a data retention order, if there is reason to assume that data that may be of significance for the clarification of the offence is deleted or changed. This is related to search of a data contained in a device and may be issued before the search is conducted. This only means an order that the data is to be maintained unchanged and does not contain a right to obtain information on the contents of a message, for example.

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

Traffic data monitoring (see answer under question 28) may be issued only when there are grounds to suspect a person of 1) an offence for which the most severe punishment is imprisonment for at least four years, 2) an offence committed with the use of the network address or terminal end device, for which the most severe punishment provided is imprisonment for at least two years, 3) unauthorized use, damage to property, message interception or computer break-in directed at an automatic data processing system and committed with the use of a network address or terminal end device, 4) exploitation of a person subjected to sex trade, solicitation of a child for sexual purposes or pandering, 5) a narcotics offence, 6) preparation of an offence committed with terrorist intent, 7) an aggravated customs offence, 8) aggravated concealment of illegally obtained goods, 9) preparation of the taking of hostage or 10) preparation of aggravated robbery.

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.*

See answer under question 15. Same applies here.

In addition, seizure must be rescinded as soon as it is no longer necessary (Section 14, Chapter 7, Coercive Measures Act). On the request of the person concerned in the matter, the court shall decide whether the seizure is to remain in force or whether the copy of the document is to be retained to be used as evidence (Section 15, Chapter 7, Coercive Measures Act). Also if the

copy of a document proves to be unnecessary or if the court decides that it is not to be retained for us as evidence, the copy shall be destroyed (Section 16, Chapter 7, Coercive Measures Act). These provisions may lead to inadmissibility of the evidence.

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: Finnish legislation does not require that certain kind of protocol concerning applicable and used technical solutions and alternatives needs to be followed.

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

***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. Finnish evidence legislation (in Act of Judicial Procedure, Chapter 17) is based on relatively free discretion what comes to various kind of evidence. The Chapter was reformed in 2014 and in the reform digitalization and electronic evidence was paid quite little attention. There are no specific rules in criminal procedure regulating the use of mobile forensic tools or AI technology in the Act of Judicial Procedure. Despite of this, in practice there has not been any significant problems in this respect that I am aware of.

***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?*

Answer: The main issue is that the criminal law cooperation and mutual legal assistance in criminal matter may vary depending on the instrument applied. The legal instruments applicable in various cases form a complex entity, which is not easy to interpret and to apply.

***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. EIO and other possibly relevant instruments are used according to their scope of application.

***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: Finnish authorities follow instructions given in Governmental Proposal 29/2017 vp (concerning the national implementation of EIO). In the proposal it is stated that EIO is applied

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

when the question is on evidence-related matters but other situations related to mutual legal assistance, like service of summons, belong to the scope of application of other instruments.

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

Answer: There are possibilities for cooperation between the private sector and the authorities set in the relevant Finnish legislation. The requirements for cooperation are set in relevant legislation. I am not aware of any existing cooperation that is not following these rules and requirements.

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: Directive 2016/680 has been implemented in Finland by an Act on the Processing of Personal Data in Criminal Matters and in Connection with Maintaining National Security (Act 1054/2018). The Act applies to the processing of personal data by competent authorities in the context of 1) preventing, detecting or investigating criminal offences or referring them for consideration of charges; 2) consideration of charges and other activities of a prosecutor in relation to a criminal offence; 3) hearing a criminal case in court; 4) enforcing a criminal sanction; 5) safeguarding against, and preventing threats to, public security in connection with activities referred to in paragraphs 1–4. If collecting e-evidence also contains gathering of personal data, the provisions of the mentioned act apply.

There are, as already indicated above, few important limitations concerning on which kind of data can be analysed and how. Firstly, search of a data contained in a device may not be directed at a confidential message in respect which telecommunications interception, traffic data monitoring and technical surveillance are applicable. Secondly, there are also relevant limitations to telecommunications interception and technical surveillance in Section 52, Chapter 10 of the Coercive Measures Act. These limitations are relate mostly to situations where a person has a right or an obligation to refuse from testimony. These limitations are, thus, mostly because of privacy

concerns and confidentiality. The coercive measures described in Chapter 10 of the Coercive Measures Act are measures the prerequisites of which are most strict because of their privacy invading character.

What comes to more general fundamental rights considerations, the probative value of forensic investigation is upon the courts to decide. Like stated above, in the Finnish judicial procedure the discretion on the probative value of a certain piece of evidence is relatively freely considered and various aspects are taken into account. Finnish courts are well aware of the case-law of the European Court of Human Rights that forms the foundation of this discretion. There are, however, not specific rules on how a certain kind of piece of evidence should be considered and how its probative value should be assessed.

There are detailed provisions on for how long information can be retained or copied. According to the Section 22, Chapter 8 of the Coercive Measures Act, concerning search of data contained in a device, if the search of the device cannot be conducted without delay, the device shall be seized. The phrase “without delay” has not been defined in legislation, but in practice it has been interpreted to cover few days. According to Section 14, Chapter 7 of the Coercive Measures Act, seizure shall be rescinded as soon as it is no longer necessary. It shall be rescinded also if no charges are brought for the underlying offence within four months of the seizure of the object, property or document. A court may, at the request of an official with the power of arrest, extend this period by at most four months at a time, if the prerequisites for seizure continue to exist and if continuing to keep the seizure in force is not unreasonable.

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?*

Answer: No.

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: Like already indicated above, there are no special rules in Finnish judicial procedure concerning evidence collected through mobile forensics. This kind of evidence are pieces of evidence among others and according to law the court shall consider the probative value of the evidence and the other circumstances thoroughly and objectively on the basis of free consideration of the evidence, unless provided otherwise in law (Chapter 17, Section 1, Subsection 2, Act on Judicial Procedure).

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: In these situations, Section 25, Subsection 3, Chapter 17 of the Act on Judicial Procedure applies. The subsection is as follows: "In other cases the court may use also evidence that has been obtained unlawfully, unless such use would endanger the conduct of a fair trial, taking into consideration the nature of the case, the seriousness of the violation of law involved in the obtaining of the evidence, the significance of the method in which the evidence was obtained in relation to its credibility, the significance of the evidence in respect of the decision in the case, and the other circumstances."

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: When Finnish evidence law is based on the principle of free consideration of evidence, the Courts are basically entitled to take this kind of evidence into account. This means that the fact that data is located outside Finland does not make it inadmissible. The fact can, however, affect the reliability of the evidence and the soundness of electronic or mobile evidence, as assessed by 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 originality and integrity or soundness of electronic or mobile evidence has been an issue that has been considered in Finnish legal literature. It has been estimated that questions on the original nature of evidence (which affects the evidential value of the piece of evidence) and integrity of evidence are more critically evaluated if the question is on electronic evidence. This may be true, but it does not in principle affect the admissibility of such evidence. This also means that alteration of evidence meant in this question may have an effect on how the courts are considering the value of the piece of evidence that is altered but alteration does not as such render the evidence inadmissible.

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: There are no specific rules on this under Finnish legislation on judicial procedure. In separate court cases the question on the soundness of this kind of evidence may actualise. If it could be shown that the evidence has been acquired by using technology that is also forensically sound, this may have an effect that strengthens the reliability and soundness of the evidence from the viewpoint of the court. This is, however, a matter of the court independently to decide.

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

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

Answer: No.

***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: I am not aware of such standardisation. Certain kind of standardisation could be achieved through the fact that there are formal requirements set in the legislation concerning the authority who is entitled to order a coercive measure. In most cases the authority entitled to decide on the measure is either an official with the power of arrest or court. This enhances consistency and secures that consideration concerning each measure in each case is carried out in a legally sound way, but does not mean such standardisation that is meant in this question.

***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: Like mentioned above, there are important restrictions to seizure and copying that mostly relate to 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: No, at least not from the Supreme Court of Finland.

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: Mobile forensic evince is not given any certain probative value in Finnish legal system. Like already stated, Finnish legislation on judicial procedure does not contain such provisions but Finnish evidence law is based on the free consideration of evidence, which means that the probative value of the evidence is thoroughly considered by the court without any specific legislative rules giving certain probative value to certain kind of evidence. There are also no rules on how to interpret mobile forensic evidence which must be complied for the evidence to be considered reliable. This is also a matter of the court to decide on the basis of free consideration of evidence. There is no general requirement that such evidence needs to be examined by an expert witness. When the members of the court in general do not necessarily possess detailed expert knowledge on mobile devices and various information systems, there is, however, a strong need for expert witnesses in this respect. The use of such witnesses is, however, not a requirement in any respect. Detailed information on how often expert witnesses are used in these cases is not available. General requirements for expert witnesses set in Act on Judicial Procedure (Section 35, Chapter 17): an expert witness shall be known to be honest and competent in his or her field and a person who is

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

connected with the case or a party in a manner that endangers his or her impartiality may not serve as an expert witness. According to my knowledge there is no centralised management of mobile forensic operations in Finland.

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

Answer: No, at least the Supreme Court of Finland has not delivered any precedents on the matter.

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: No. In some cases the courts may have to assess whether the methodology, tools or techniques used in mobile forensics are reliable. In these situations expert witnesses are presumably important and statements of expert witnesses may crucially affect the court's considerations on the reliability of evidence.

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: No, at least the Supreme Court of Finland has not delivered any precedents on the matter.

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?*

Answer: No. General provisions and principles on fair trial apply.

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: No. The training is not required but there are various training possibilities available for judges and prosecutors relating to mobile forensics.

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: No.

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: In the Finnish judicial system the procedural rights of each participant are closely formulated in line of the requirements set in European Convention of Human Rights, case-law of the European Court of Human Rights, EU Charter of Fundamental Rights and relevant EU directives on procedural rights, and also in the Constitution of Finland. The procedural rights inherent to different participants in criminal procedure thus contain all relevant procedural rights guaranteed in these fundamental and human rights instruments and in case-law interpreting them.

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

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: No. There are, however, general guidance on the use of coercive measures given by the Prosecutor General of Finland. According to these somewhat general instructions, the prosecutor is responsible for the law-abiding, effective and appropriate use of the coercive measures during the whole criminal process. This applies also to coercive measures that are used in obtaining electronic evidence. In addition, general principles and requirements and special requirements on the use of coercive measures apply.

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.*

Answer: No. Like stated above, Finnish evidence law is based on the free consideration of evidence.

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: Evidence obtained via mobile forensics is basically assessed like any other evidence, on the basis of the free consideration of evidence. As it is stated in Section 1, Subsection 2, Chapter 17, Act of Judicial Procedure: The court, having considered the evidence presented and the other circumstances that have been shown in the proceedings, determines what has been proven and what has not been proven in the case. The court shall consider the probative value of the evidence and the other circumstances thoroughly and objectively on the basis of free consideration of the evidence, unless provided otherwise in law.

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: In the Finnish criminal process a broad view to publicity, especially in relation to the parties of the process, has been adopted. After the initiation of the criminal investigation a party has the right to obtain information on matters that have led to or become apparent in the criminal investigation and on the documentation in the criminal investigation that may or could have affected the consideration of his or her matter (Section 15, Subsection 1, Chapter 7 of the Criminal Investigation Act). This also means that the defendant and his/her defender have the right to access and make copies of the acquired mobile evidence of the case. Equality of arms requires that this provision is interpreted broadly and the defendant should in principle be given also relevant information on how forensic evidence has been gathered and on the technical tools and procedures used in creating and obtaining relevant data. There is no case law on this matter.

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: Criminal Investigation Act contains a provision on the right to refuse to testify in pre-trial stage (Section 8, Chapter 7). The provision contains several situations in which the right to refuse to testify may actualise and most of the situations are related to the protection of the privacy of the witness.

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.*

Answer: Section 15, Subsection 1, Chapter 7 of the Criminal Investigation Act, applies also to the victim of the case, which means that the victim also has a broad right to obtain evidence acquired in the case.

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.