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: Indication of length of answer: one line.

Department of Law, Umeå University. Assistant professor.

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

Answer: Indication of length of answer: one line.

Umeå, Sweden.

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: Indication of length of answer: couple of lines.

There is no general legally defined term for a "mobile device". However, Code of Judicial Procedure (Sw. rättegångsbalken (1942:740)) chapter 23, section 9 a, enables seizure of *electronic communication device* (Sw. "elektronisk kommunikationsutrustning") under certain circumstances, but this also includes e.g. stationary computers (see also Code of Judicial Procedure, Chapter 27, Section 19. In Traffic Decree (Sw. trafikförordningen (1998:1276)) – which is a penal law legislation – chapter 4 section 10 e the word "mobile phone" is mentioned, but there is no definition of that word.

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?*

Scenario A). *In the context of a search of premises (or frisk serach).* The legal position is not clear in this respect and there is no clear legislation or precedents. However, the Swedish Code of Judicial Procedure Chapter 28 Section 8 gives some support for the interpretation that objects – such as mobile devices – are allowed to be searched without seizing it. My interpretation is that the condition for this is that the search is of short duration, that the mobile device is not moved and that the aim of the investigation is to see whether the device is relevant to seize or not. Today most scholars consider that it is not allowed to replace a seizure with only a search. (There are other conditions that must be fulfilled for a search of premises or a frisk search, see question 17 below. A search of the premises is needed when the mobile device is located e.g. inside a house, a car or a bag, Code of Judicial Procedure Chapter 27 Section 1. A frisk search is needed when the mobile device is located near a person, e.g. in his or her clothes or hands, see Code of Judicial Procedure Chapter 27 Section 11.)

Scenario B). *After a court order on Covert Data-Reading.* There are four conditions for a permission to perform a covert data-reading during a preliminary investigation according to Law of Covert Data Reading (Sw. lag (2020:62) om hemlig dataavläsning), Section 3 and 4: (1) the covert data-reading must be of exceptional importance for investigating a crime, (2) the

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

investigated crime must be severe and, (3) the mobile phone must be used by a person who is suspected on reasonable grounds and (4) the data-reading must be proportionate.

Scenario (C) Secret eavesdropping and Scenario (D) secret surveillance. I will not deal with these situations, as these coercive measures are not used to investigate already existing information in a mobile device.

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?*

Scenario A. If there is a prohibition to seize, you cannot search a premise in order to find the object either, see question 19 below.

Sceanario B. There are a number of exceptions from the possibility to perform covert data-reading according to Law of Covert Data-Reading, Section 11, e.g. activities operated by medical doctors, nurses and lawyers.

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

Scenario A. This is not regulated, see question 23.

Scenario B. Yes, according to Law of Covert Data-Reading, Section 22.

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

Sceanario A. The information can probably only be read. Scholars recommend to first seize the mobile device, then copy the information and last – possibly – annul the seizure.

Sceanario B. According to Law of Covert Data-Reading, Section 1, the information can be read or recorded.

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

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

Scenario A. No, the mobile device can be read/investigated in order to determine whether the mobile device is relevant to seize irrespective of a consent.

Scenario B. No.

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

Scenario A. No, see question 21 below.

Scenario B. No, there is no such provision in Law of Covert Data-Reading.

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

Scenario A. If the investigation shows that the mobile device is not relevant to seize, there is no rule that stipulates that the owner/possessor must be informed, but still it could be suitable to do so. However, if a search takes place in e.g. a house the police have to draw up a protocol and the owner /possessor has a right to have certificate of the search, according to the Swedish Code of Judicial Procedure Chapter 28 Section 9. In addition, the people who live in the house also have a right to be attend at the search of the premises, see Code of Judicial Procedure Chapter 28 Section 7.

Scenario B. No, the data-reading is covert, which means that the owner/person in possession of the mobile must not be informed.

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

Scenario A. Often search of the premises (if the mobile phone is e.g. lying inside a house) or a frisk search (if a natural person is carrying the mobile device) is needed to search a mobile phone in order to decide whether to seize it. Some scholars argue that the mobile device itself is a *concealed storage place* (Sw. "slutet förvaringsställe"), which requires a search order to be accessible even if you e.g. find the mobile telephone on the street. See further question 17 below.

Irrespective of a search of the premises or a frisk search is needed there are corresponding rules about who can order a search. According to Code of Judicial Procedure Chapter 28 Section 4

and 13 the prosecutor and the police that leads the preliminary investigation can order a search; in some cases the court orders a search, but this occurs very rarely. If the situation is urgent a single policeman can order a search according to Code of Judicial Procedure Chapter 28 Section 5 and 13.

Scenario B. The court, according to Law of Covert Data-Reading, Section 14. However, the prosecutor can under certain conditions order a temporarily covert data-reading pending the court´s decision, Law of Covert Data-Reading, Section 17.

12. *Does it matter whether this person is the accused or witness/third party or the victim?*
Scenario A. If a search of the premises or a frisk search is needed, there are different rules regarding these two coercive measures for a person who is suspected on reasonable grounds and another person, see Swedish Code of Judicial Procedure Chapter 28, Section 1 and 11.

Scenario B. As mentioned in question 4 the mobile phone must be used by a suspect on reasonable grounds.

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.*
Scenario A + B. If data is known or suspected to reside outside the country Swedish criminal investigators cannot act on their own, but need help from other countries. Aside from EIO and MLATs there are also other conventions – such as The European Convention of Mutual Legal Support in Criminal Cases from 1959 – some bilateral agreements between Sweden and some other countries – Bahamas, Canada, Finland, Hong Kong, Switzerland, United Kingdom and United States of America – and the regulations in other countries that might allow information to be shared.

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

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

Scenario A. Yes. If a search of the premises or a frisk search is needed, there must be a suspicion that a crime that can lead to imprisonment has been committed, see Swedish Code of Judicial Procedure Chapter 28, Section 1 and 11.

Scenario B. As mentioned in question 4, the crime must be severe, e.g. crimes for which the crime punishment is 2 years imprisonment or more.

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.*

Scenario A and B. If applicable national rules (in Code of Judicial Procedure or Law of Covert Data-Reading) are not followed probably the evidence will be admissible, but it might affect the value of evidence in some situations. According to Swedish Law the principle of "free production of evidence" means that all evidence is admissible. For instance, Code of Judicial Procedure Chapter 28, Section 8, states that only the court, the prosecutor and the police that leads the preliminary investigation are allowed to search the objects (e.g. mobile devices). If this rule is not followed – e.g. the mobile phone is investigated by a single policeman – the evidence still probably would be admissible; compare The Surpreme Court in NJA 1986 s. 489 regarding body search. There are no explicit rules about this.

If the right to a fair trial according to article 6 of the European Conventions on Human Rights and Freedoms is not followed the answer might be different. In such case however, the Swedish Surpreme Court often has chosen other reactions to the violation than to declare the evidence admissible, e.g. to state that it is not possible to bring a prosecution (NJA 2007 s. 1037) or to reduce the penalty (NJA 2011 s. 638).

However, there is one exception to the above mentioned in Law of Covert Data-Reading Section 23. According to this provision it is not allowed to use the technique to read or record

other information than mentioned in the court´s decision. If such information is read or recorded criminal investigators must not use this information in a criminal investigation, i.e. the information is inadmissible.

Mobile device seized

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

Yes. In Swedish Law there are a number of rules that allow the police and other officials to seize objects. In the following, I will focus on the general rules in Code of Judicial Procedure, Chapter 27, which are very commonly applied by criminal investigators. These rules are applicable when police investigate an already committed crime and other more specific rules often are based on the rules in Code of Judicial Procedure, Chapter 27.

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

There are two conditions for seizing a mobile device according to Code of Judicial Procedure, Chapter 27, Section 1: (1) the seizure must be relevant for investigating a crime and (2) the seizure must be proportionate. In addition, according to the preparatory works, all coercive measures – seizure included – must be needed; that means – in my opinion – that a seizure must be (1) necessary, (2) effective and (3) there is no lighter form of measure than the seizure that might have the same effect.

However, another requirement is that the mobile device is accessible. The mobile device is accessible e.g. if the police find it lying in the street, and in that case only the conditions mentioned in the previous paragraph must be fulfilled. If the mobile device is not accessible other coercive measures must be used to make it accessible – above all a search of the premises (if the mobile phone is e.g. lying inside a house) or a frisk search (if a natural person is carrying the mobile device). To perform these measures there are additional conditions that must be fullfilled – e.g. there must be a suspicion that a crime that can lead to imprisonment has been committed. However, some scholars argue that the mobile device itself is a *concealed storage place* (Sw. "slutet förvaringsställe"), which requires a search order to be accessible.

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

According to Code of Judicial Procedure Chapter 27 Section 4 the prosecutor and the police that leads the preliminary investigation can order a seizure. If the situation is urgent a single policeman can order a seizure. In addition, people who perform e.g. a search or frisk search with legal right are allowed to seize a mobile device and other objects. According to Code of Judicial Procedure Chapter 27 Section 5 the court is allowed to seize a mobile when it is accessible – e.g. during a main hearing – but this occurs very rarely.

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

Yes, a seizure means that the mobile device can be searched, information, copied, etc. This follows indirectly from Code of Judicial Procedure Chapter 27 Section 12. However, according to the same section of law mobile phones that are owned/possessed by private subjects can only be searched by the court, the prosecutor or the police that leads the preliminary investigation.

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?*

There are a number of exceptions from the possibility to seize objects in Code of Judicial Procedure Chapter 27 Section 2 and 3, e.g. if a document contains entrusted information between an attorney and his/her client or messages between the suspect and his/her family. If there is such a prohibition to seize, you cannot search a premise to find the object either.

The Swedish Surpreme Court has in NJA 2015 s. 631 stated that these prohibitions to seize are also applicable regarding electronic devices. If the file sought for can be presumed to contain information that is prohibited to seize, the electronic device cannot be seized at all. If there are other files than the file sought for that contains such information there is no such prohibition to seize the device. The Surpreme Court has also stated that the police that looks for a certain file is not allowed to open other files. In addition, The Swedish Prosecutor General has stated in JK 2007-12-19, dnr 6372-07-31 and 6373-07-31, that the search in a computer should be directed

and limited and that the computer shold be immediately shut down if the police bump into information that is covered by a prohibition to seize.

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

Most scholars consider that a consequence of the situation that a person that hands over an object on his or her own initiative, is that there is no need for a search or a frisk search to be able to seize the object. However, even if the object is voluntarily handed over, most scholars consider that the object should be seized.

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

No, not according to a decision from the Swedish Parliamentary Ombudsman, see JO 2020-06-30, dnr 6489-2018, who argues that there is no legal support for doing this (the case concerns taking of finger prints, but there is no legal support for this measure according to the regulation regarding seizure either).

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

According to the Code of Judicial Procedure Chapter 27, Section 11, the owner/person in possession of the object must be informed if he or she is not present when the object is seized; however, some sholars argue that this is also the case when he or she is present. According to a sholar it is enough that the police orally inform the owner/possessor what objects that will be seized. In addition, according to the Swedish Parliamentary Ombudsman in JO 1975/76 s. 156, the police have to inform how the objects will be documented and that there is a right to demand judicial review.

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

This is not regulated, and the legal position is unclear. Probably it is allowed to use measures that simply bypass already existing security but not allowed to use such techniques – e.g. viruses – that alters the contents in the information device.

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

It does not matter if seizure is the only coercive measure that is required – the rule in Swedish Code of Judicial Procedure Chapter 27, Section 1, is applicable irrespective of whom the mobile device belongs to (see question 17 above). If a search of the premises or a frisk search is needed however, there are different rules regarding these two coercive measures for a person who is suspected on reasonable grounds and another person, see Swedish Code of Judicial Procedure Chapter 28, Section 1 and 11.

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 known or suspected to reside outside the country Swedish criminal investigators cannot act on their own, but need help from other countries. Aside from EIO and MLATs there are also some bilateral agreements between Sweden and some other countries — Bahamas, Canada, Finland, Hong Kong, Switzerland, United Kingdom and United States of America – and the regulations in other countries that might allow information to be shared.

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?*

It is not legally possible to get access to such information. In this situation however – according to a forensic examiner – it is possible to secure the evidence until the location is determined.

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?*

If that is the case, it might be legally possible to access data in the cloud in other ways (if these ways are technically possible). One way is to get data from the Service Provider (see question 28). Sometimes it is even possible to access data in the Cloud from an open web page.

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?*

There is a special regulation in Law of Electronic Communication (Swedish lag (2003:389) om elektronisk kommunikation) about access to data kept by a Service Provider alongside the

regulation of seizure in Code of Judicial Procedure Chapter 27. The first mentioned law Chapter 6, Section 22, gives criminal investigators – under certain conditions – access to some information concerning an electronic message that the Service Provider (operator) has access to. This transfer of information however, is not performed upon a Court order, but the Service Provider self has to decide to transfer the information.

My opinion is that criminal investigators can get access to data kept by a Service Provider in two alternative ways – either they search the premises of the Service Provider and seize the server, or they ask the Service Provider to leave them the information. However, the legal possibilities to get access to data kept by a Service Provider is limited. In criminal investigations the Law of Electronic Communication nowadays only gives access to information about the subscription (and IP address). In addition, searches according to the Code of Judicial Procedure Chapter 28 are often considered disproportionate.

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

It does not matter if seizure is the only coercive measure that is required – the rule in Swedish Code of Judicial Procedure Chapter 27, Section 1, is applicable irrespective of the severeness of the crime committed. If a search of the premises or a frisk search is needed however, there must be a suspicion that a crime that can lead to imprisonment has been committed, see Swedish Code of Judicial Procedure Chapter 28, Section 1 and 11.

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 the answer in question 15. Another thing is that – if the seizure still is in progress – the court is able to annul the seizure if all the conditions not are fulfilled, see Code of Judicial Procedure Chapter 27, Section 6.

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

No, there are no such rules and – as far as I know – no guidelines either. However, there is software – approved by the Police authorities – which contains instructions about this. According to a forensic examiner they usually change the adjustments in the mobile phone, but not the user data.

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

No, not as far as I know.

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

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

In the cases when mobile devices are involved in crimes across geographical boundaries different problems arise. One problem is that there are different rules in different countries and it is difficult to know what rules that are applicable in a case. Sometimes it is not possible according to the laws of the foreign country to receive the information that the criminal investigators are interested in and sometimes there are local judges who do not want to assist. Another problem is the time delay in some countries. However, there are handbooks functioning as manuals and Swedish criminal investigators can receive assistance from Eurojust, Europol and European judicial networks.

Regarding the awareness of the forensic examiner – according to a prosecutor – the answer may be no. The forensic examiner does the technical things – lika emptying the mobile phone – while the criminal investigators analyze the information.

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

There are two handbooks – one about the EIO and one about legal support – written by the prosecutor´s office that contains guidance whether to apply the EIO or legal support.

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

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

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

The importance of MLATs – such as the European Convention on Mutual Assistance in Criminal Matters – has been reduced, but in certain situations there are still reasons to apply MLSATs instead of EIO.

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

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

Sometimes it is necessary to hire private experts on IT forensics.

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

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

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

- *Data protection concerns (Law Enforcement Directive 2016/680 and implementing national law)*

  In Sweden the Law Enforcement Directive is implemented through Crime Data Law (Sw. brottsdatalag (2018:1177)). This law contains several provisions about treatment of personal information – including the processing of such information – but there is no specific regulation regarding the situation when data has been accessible through mobile forensics.
- *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)*
- This is not regulated in law. The Surpreme Court however, has in NJA 2015 s. 631 stated that the investigator that looks for a certain file is not allowed to open other files. In addition, The Swedish Prosecutor General has stated in JK 2007-12-19, dnr 6372-07-31 and 6373-07-31, that the search in a computer should be directed and limited and that *a computer* should be immediately shut down if the police bump into information that is covered by a prohibition to seize. Both The Surpreme Court and the Prosecutor General consider that the owner/possessor has the right to attend during the analysis. See also question 19 above; I think it is hard to draw a clear-cut line between investigation and analysis.

  According to Law of Covert Data-Reading Section 23 it is not allowed to use the technique to read or record other information than mentioned in the court´s decision (in case of a court order on covert data-reading).

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

- *What information can be retained/copied? For how long?*

  The original information can be retained as long as the seizure endures. There is no time limit for seizures, but they have lasted for years in some cases; the seizures however, must be proportionate.

  The copying of seized objects is not regulated, but scholars consider that all information that a lawfully seized mobile device contains can be copied (compare question 19 above). The time of retention depends on whether the preliminary investigation is closed (5 years) or if the case is decided (6 months) according to the regulations of the National Archives regarding retention and sorting out RA-MS 2019:32 (these regulations aim at copies of seized electronic documents that have been produced by forensic analysis programmes).

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

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

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

No. However, if it – in the context of a covert data reading – would be discovered information regarding another crime than the one the court order of covert data-reading is based on, a preliminary investigation must not be initiated unless the discovered crime is severe or there are special reasons. However, there is no prohibition *to use* the information. See Law of Covert Data-Reading Section 28 and Code of Judicial Procedure Chapter 27 Section 23 a.

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

The criteria are the same. As elaborated in question 15, the principle of "free production of evidence" means that all evidence are admissible and that there are few exceptions to this principle.

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

Evidence from mobile forensics can still be submitted to court. See question 15 and the example given regarding Code of Judicial Procedure, Chapter 27, Section 8.

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

No, the data is admissible. Another question is if it is legally possible to get access to this information. The evidentiary requirement is not clear.

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

No, it does not render the evidence inadmissible but it might effect the value of evidence.

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

No.

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

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

No, none of the cases from the Surpreme Court regarding mobile devices deals with this question, see NJA 2018 s. 844, NJA 2016 s. 490, NJA 2014 s. 14, NJA 2011 s. 466, NJA 2009 s. 819, NJA NJA 2007 s. 431, NJA 2004 s. 336.

***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*

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

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

No.

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

No.

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: Indication of length of answer: 3+ paragraphs.

No, none of the cases from the Surpreme Court regarding mobile devices deals with this question, see NJA 2018 s. 844, NJA 2016 s. 490, NJA 2014 s. 14, NJA 2011 s. 466, NJA 2009 s. 819, NJA NJA 2007 s. 431, NJA 2004 s. 336.

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?*

According to the principle of free evaluation of evidence the judge is free to evaluate all sorts of evidence. There is no case law where The Surpreme Court has given mobile forensic evidence a certain probative value, see see NJA 2018 s. 844, NJA 2016 s. 490, NJA 2014 s. 14, NJA 2011 s. 466, NJA 2009 s. 819, NJA NJA 2007 s. 431, NJA 2004 s. 336.

- *Are there rules on how to interpret mobile forensic evidence or requirements which must be complied with for the evidence to be considered reliable?*
  No.
- *Must such evidence be examined by an expert witness?*
  No, there are no formal requirements; the parties present the evidence they want according to the principle of free production of evidence.
- *If not obligatory, is this a common practice?*
  According to a judge, it is common in some cases – such as child pornography offence or certain serious crimes (e.g. murder) – but not in others.
- *What are the requirements for experts (experience, independence, training, etc.)?*
  There are no formal requirements. The experts are often civil employees from the Police authorities or employees from the Swedish National Forensic Centre (see next question below). They are often system scientists with long experience.
- *Is there a centralised management of mobile forensic operations in your jurisdiction to ensure the work is compliant with standards and can be presented in court in a consistent manner?*

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

There is the Swedish National Forensic Centre, NFC. NFC is an independent expert organization within the Swedish Police Authority with an overall responsibility for forensics. Its main task is to conduct forensic investigations and analyzes on behalf of the judicial authorities. Its mission is to integrate, consolidate and streamline the national forensic services to meet society's need, see https://nfc.polisen.se/en/about-nfc/our-mission/.

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

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

No, none of the cases from the Surpreme Court regarding mobile devices deals with this question, see NJA 2018 s. 844, NJA 2016 s. 490, NJA 2014 s. 14, NJA 2011 s. 466, NJA 2009 s. 819, NJA NJA 2007 s. 431, NJA 2004 s. 336.

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

No.

***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.*

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

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

No, none of the cases from the Surpreme Court regarding mobile devices deals with this question, see NJA 2018 s. 844, NJA 2016 s. 490, NJA 2014 s. 14, NJA 2011 s. 466, NJA 2009 s. 819, NJA NJA 2007 s. 431, NJA 2004 s. 336.

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: Indication of length of answer: couple of paragraphs.

No, none of the cases from the Surpreme Court regarding mobile devices deals with this question, see NJA 2018 s. 844, NJA 2016 s. 490, NJA 2014 s. 14, NJA 2011 s. 466, NJA 2009 s. 819, NJA NJA 2007 s. 431, NJA 2004 s. 336. However, there are some general rules – not only applicable in case of evidence extracted via mobile forensics – in the Code of Judicial Procedure: According to Chapter 23, Section 18 a the suspect and his or her defender have a right to take part of the investigation (party insight) and also a right to ask that the investigation is completed. According to Chapter 35, section 5 and the principle of free production of evidence the suspect and the defender can put forward their own evidence.

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

No, there is no specific training required by law. All prosecutors however, get at least some education about evidence coming from an IT environment. Swedish judges in the general courts are generalists, but there are some (a few?) prosecutors and lawyers who are experts in these matters.

***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?*

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

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

No, but the crime will be statute-barred after some years, see the Swedish Code of Crime (Sw. brottsbalken (1962:700)) Chapter 35.

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

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

The court. In a Swedish context, we usually do not talk about procedural rights regarding this participant. However, the court has the right to formal and material direction of proceedings. Formal direction of proceedings is the court´s right to direct the course of the trial, i.e. the time and turn order (Code of Judicial Procedure Chapter 43 Section 4 Paragraph 1 and Chapter 46 Section 4 Paragraph 1). Material direction of proceedings is the court´s right to guide the parties regarding the process material (Code of Judicial Procedure Chapter 43 Section 4 Paragraph 2 and Chapter 46 Section 4 Paragraph 2).

The prosecutor. In a Swedish context, we usually do not talk procedural rights regarding this participant. However, according to Code of Judicial Procedure Chapter 35 section 5 and the principle of free production of evidence the prosecutor has a right to put forward any evidence they want. The prosecutor also has the right to decide to use several coercive measures such as search and seizure (see questions 11 and 17 above).

The defendant. The defendant has several rights according to the Code of Judicial Procedure. (a) *Pre-Trial phase*. When the defendant is reasonably suspected he or she has a right to be notified about the crime (Chapter 23, section 18) and the interrogator must – according to the Preliminary Investigation Announcement (Sw. förundersökningskungörelsen (1947:948)) Section 12 – point out that he or she has the right to apply to a defender according to Chapter 21 section 3 and 3 a. According to the Code of Judicial Procedure Chapter 23 Section 18, the defendant has a right to get access to the acquired evidence during the preliminary investigation, *if this does not harm the*

investigation. When the preliminary investigation is finished, according to Code of Judicial Procedure Chapter 23 Section 18 a, this right is without exception. According to the last mentioned provision, the defendant also has the right to ask the prosecutor to complete the investigation; in addition, according to Chapter 23 Section 18 b an interrogation or other investigation shall take place if the defendant or defender requests this, if it is supposed to be relevant for the preliminary investigation. According to Chapter 23 Section 10 the defendant has the right to have his or her defender present when the defendant is questioned or there are other interrogations on the defendant´s demand; during other interrogations the defendant has the right to have his or her defendant present *if this does not harm the investigation*. After the defendant having been prosecuted he or she also gets copies of the preliminary enquiry report according to Code of Judicial Procedure Chapter 21 Section 21 a. The defendant also has the right to remain silent (according to basic principles and the fact that there is no regulation that ordains the defendant to speak), and must be notified about this according to the Preliminary Investigation Announcement Section 20. (b) *Trial phase*. The defendant has the right to remain silent, see above. According to Code of Judicial Procedure Chapter 35 section 5 and the principle of free production of evidence the defendant has a right to put forward any evidence he or she wants. In addition, he or she has the right to ask questions about/to evidence presented by the prosecutor or victim.

The witness. In a Swedish context, we usually do not talk procedural rights regarding this participant. However, according to the Code of Judicial Procedure Chapter 36 Section 24, the witness has the right to certain economic compensation for his or her appearance. There are also some rules that aims at protect the witness, e.g. the possibility for the court according to Code of Judicial Procedure Chapter 36 Section 18 to – under certain circumstances – ask the defendant to leave the court room during the testimony. Witnesses have no more extended right to insight in the investigation than the public.

The victim. The victim has a right to be represented by the prosecutor or a counsel for an injured party (when certain crimes have been committed), according to the Law on Counsel for an Injured Party (Sw. lagen (1988:609) om målsägandebiträde). (a) Pre-trial phase. According to the

Preliminary Investigation Announcement Section 13 a–13 e the victim has a right to be asked and notified about certain circumstances, e.g. that the prosecutor has decided to prosecute. According to Chapter 23 Section 10 the wictim has the right to have his or her counsel present when the victim is questioned. If the prosecutor does not want to prosecute the wictim has a right to prosecute according to the Code of Judicial Procedure Chapter 20 Section 8. (b) Trial phase. According to Code of Judicial Procedure Chapter 36 Section 18, there is a possibility for the court to – under certain circumstances – ask the defendant to leave the court room when the victim is questioned during the trial. During the trial the victim has – according to the Code of Judicial Procedure Chapter 20 Section 8 – the right to assist the prosecution, e.g. present evidence and question witnesses; acccording to the same provision the victim also has the right to appeal. The wictim also has the right to economic compensation for the damage he or she has suffered, e.g. according to the Law of Crime Damage (Sw. brottsskadelagen (2014:322)).

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: Indication of length of answer: couple of paragraphs.

There is some guidance in a FAQ (frequent asked questions) – written by the prosecutor´s office and available for prosecutors – about how to deal with mobile forensics and evidence, e.g. how to copy the material and how to avoid that new messages arrive after that the mobile phone has been seized.

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.*

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

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

There is no judicial control in a strict sense, i.e. that the court controls the approaches and methods used. However, officials using bad methods can get criticism from the Parliamentary Ombudsman or – in severe cases – get prosecuted for official misconduct. Another thing is that a person who suffers from a seizure according to Code of Judicial Procedure Chapter 27 Section 6 has a right to request a judicial review from the court, but in that case only the conditions for seizure are reviewed. There is no case law.

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

There is no cases from the Surpreme Court regarding mobile devices deals with this question, see NJA 2018 s. 844, NJA 2016 s. 490, NJA 2014 s. 14, NJA 2011 s. 466, NJA 2009 s. 819, NJA NJA 2007 s. 431, NJA 2004 s. 336. According to a judge the work of the mobile forensics if often not questioned, but there are other issues that must be assessed – e.g. it is not disputed that the suspect´s mobile phone contains child pornography, but the suspect claims that somebody else has handled his or her mobile phone.

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: Indication of length of answer: couple of paragraphs.

According to the Code of Judicial Procedure Chapter 23 Section 18, the defendant has a right to get access to the acquired mobile evidence during the preliminary investigation (pre-trial phase), *if this does not harm the investigation*. When the preliminary investigation is finished, according to Code of Judicial Procedure Chapter 23 Section 18 a, this right is without exception; after the defendant is prosecuted he or she also gets copies of the preliminary enquiry report according to Code of Judicial Procedure Chapter 21 Section 21 a (see also JO 1996/97 s. 74). If the defendant wants get information on the process used to acquire mobile forensic evidence, they can ask the expert witness/the person who has acquired the data in conjunction with the questioning of the witness during the main hearing; if the prosecutor has not summoned such a witness the defender can summon a witness of his or her own. There is no case law regarding this.

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: Indication of length of answer: couple of paragraphs.

The witnesses have no right to be anonymous, unless they have protected identity. As mentioned above (question 19) the search in mobile data should be directed and limited. There are no particular requirements for witnesses regarding their capability to testify in terms of mobile forensics, but as mentioned in question 48 the experts are often employees from the Police authorities or the Swedish National Forensic Centre. There is no case law regarding this.

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: Indication of length of answer: couple of paragraphs.

Regarding how the victim´s rights are ensured during both the pre-tral and trial phase of the proceedings, see question 55 above. As mentioned above (question 19) the search in mobile data should be directed and limited. As mentioned in question 55 above the victim has – according to the Code of Judicial Procedure Chapter 20 Section 8 – the right to assist the prosecution, which means that he or she has the right to present evidence obtained via mobile forensics and to ask questions about such evidence presented by the prosecutor or defendant. There is no case law regarding this.

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.

These questions are not so regulated in Sweden and sometimes the legal position is unclear. The Swedish principle of free production of evidence has resulted in that some of my answers are very short.