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

IMPORTANT TO READ BEFORE ANSWERING THE QUESTIONNAIRE:

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

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

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

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

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

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

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: Libertas Advocaten (officially: Libertas Corporate Defense Lawyers), specialized in corporate criminal defense, fraud and white-collar crime.

   This questionnaire was answered by mr. P.C. (Paul) Verloop, lawyer and part-time judge in the Amsterdam Court of Appeal, with the assistance of mr. Gert-Jan van Olst, professional support lawyer.

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

   Answer: Rotterdam, The Netherlands

   Introductory remark

   The Dutch Code of Criminal Procedure (hereinafter: CPC) is being thoroughly revised and updated ('Modernisering Wetboek van Strafvordering'). The proposed revision has been drafted by the Ministry of Justice and Security and the draft has been published last week (https://www.rijksoverheid.nl/documenten/publicaties/2017/11/13/documenten-modernisering-wetboek-van-strafvordering). If applicable we will revert to this draft in this questionnaire. The entry into force of the proposal is not foreseen before 2026.

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: There is no specific legally defined term for a "mobile device". A mobile device is considered to be a 'computerised device and system' ('geautomatiseerd werk') as defined in section 80sexies of the Dutch Criminal Code (hereinafter: DCC). Section 80sexies reads: *"Computerised devices and systems" shall be understood to mean a facility for the storage, processing and transfer of data by electronic means.*

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

This includes all kind of devices capable of saving, processing and transferring data, like: a tablet, laptop, smartphone, computer, navigation devices, ect, and electronic data carriers which include objects that can only save data and need other devices to perceive the data stored, like: a hard drive, usb-stick of memory card, etc.

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

Section 1: Criminal procedure when searching/reading mobile devices, seizing mobile devices and for acquisition of data on mobile devices

Question: *Mobile devices (e.g. a smartphone) may enter investigations in a variety of scenarios. A suspect or a witness may have a smartphone on them during questioning or at the scene, mobile devices may be found during the search of a home or other premises, a suspect caught in the act may have a mobile device in use etc. We want to know for all these scenarios (and others you may be able to identify) what the applicable national rules are, namely answering the following questions:*

Mobile device not seized

4. *Under what circumstances can a mobile device be read or searched without seizing it?*

Answer: According to section 134 CPC "seizure of any object" shall be understood to mean the taking or holding possession of that object for the purpose of the criminal proceedings. According to section 94 CPC all objects that may serve to reveal the truth or demonstrate unlawfully obtained gains shall be liable to seizure and according to sections 95 and 95 CPC any investigating officer can seize all objects (including mobile devices).

Two things are important for that matter. First, seizure in itself is no more than the act of taking possession of an object, without any formalities. After an object is seized, there are formalities to be taken into account. Second, as a result of the case-law of the Supreme Court (Hoge Raad), there is a very limited number of situations in which irregularities during an investigation can lead to exclusion of evidence. Exclusion of evidence is only possible if the irregularities occurred in the investigation leading to the prosecution of a suspect, when the irregularities breached the suspects rights and when the use of evidence obtained as a result of unlawful actions by investigating officers would result in a breach of the right to a fair trial.[1]

[1] ECLI:NL:HR:2004:AM2533 and ECLI:NL:HR:2013:BY5321.

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

Recent studies showed that police officers sometimes search a phone without officially seizing it, e.g. when they are at the crime scene and they check whether the information on the phone is worth seizing. In most cases where the device is read or searched the owner of the device is asked for permission.

There is no legal basis for reading or searching a mobile device without seizure.

5. *Are there any limits to this search (e.g. core area of private life, privacy limits, limits defined by the crime, limits defined by the order/warrant)? If so, how precise are these/must these be defined?*
   Answer: There is no legal basis for reading or searching a mobile device without seizure.

6. *Is it allowed to use technical tools to bypass security?*
   Answer: There is no legal basis for reading or searching a mobile device without seizure.

7. *Can information be copied or only read at this stage?*
   Answer: There is no legal basis for reading or searching a mobile device without seizure.

8. *Is consent of the owner/person in possession of the mobile device necessary?*
   Answer: Since there is no legal basis for reading or searching a mobile device without seizure, the only possibility to read or search the mobile device without seizure would be after obtaining permission by the owner or person in possession of the mobile device.
   That being said: the consequences of the lack of consent will differ. When the mobile device of a deceased victim of a crime is investigated, there will be no consequences. When a suspect is forced to unlock the device without seizure there might be consequences.

9. *Can the owner/person in possession of the mobile device be forced to unlock the device?*
   Answer: There is no legal basis for reading or searching a mobile device without seizure.

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

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

Answer: There is no legal basis for reading or searching a mobile device without seizure.

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

Answer: There is no legal basis for reading or searching a mobile device without seizure.

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

Answer: There is no legal basis for reading or searching a mobile device without seizure.

13. *What about data stored in the Cloud, what is the procedure to access/read this data if it is known or suspected to reside outside your jurisdiction? Is international cooperation like the European Investigation Order (hereinafter: EIO) or Mutual Legal Assistance Treaties (hereinafter: MLAT) the only route or do other options exist? Please elaborate.*

Answer: Since there is no legal basis for reading or searching a mobile device without seizure it is not possible to access data stored in the Cloud. However, according to Section 126nf CPC in the case of suspicion of a serious offence as defined in section 67(1) CPC (offences which carry a statutory term of imprisonment of at least four years and certain other offences specifically mentioned), which serious offence in view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of law and order, the public prosecutor may, if urgently required in the interest of the investigation, request the person, who may be reasonably presumed to have access to data, to provide said data. This request may only be made following prior written authorisation to be granted by the examining magistrate on application of the public prosecutor.

If it is known that the data resides outside the jurisdiction such a request can only made via an EIO of MLAT. However, e.g. Microsoft retains a Dutch law firm that handles requests pertaining to Hotmail-data. The company tends to voluntarily comply with the request. Therefor a MLAT is no longer needed.

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

Answer: A request can only be made in case of suspicion of a serious offence.

15. *Does not following the applicable rules always lead to inadmissibility in court of the evidence in this scenario? If not, please elaborate on exceptions and relevant conditions.*

Answer: According to Section 359a CPC the Court may, if it appears that procedural requirements were not complied with during the preliminary investigation which can no longer be remedied and the law does not provide for the legal consequences thereof, determine that:

a. the length of the sentence shall be reduced in proportion to the gravity of the non-compliance with procedural requirements, if the harm or prejudice caused can be compensated in this manner;

b. the results obtained from the investigation, in which there was a failure to comply with procedural requirements, may not be used as evidence of the offence as charged in the indictment;

c. there is a bar to the prosecution, if as a result of the procedural error or omission there cannot be said to be a trial of the case which meets the principles of due process.

In the application of a remedy the Court shall take into account the interest served by the violated rule, the gravity of the procedural error or omission and the harm or prejudice caused as a result of said error or omission.

According to the case-law of the Supreme Court exclusion of evidence is only possible if the irregularities occurred in the investigation leading to the prosecution of a suspect, when the irregularities breached the suspects rights and when the use of evidence obtained as a result of unlawful actions by investigating officers would result in a breach of the right to a fair trial.[2]

[2] ECLI:NL:HR:2004:AM2533 and ECLI:NL:HR:2013:BY5321.

Mobile device seized

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

Answer: Yes, according to section 94 CPC all objects that may serve to reveal the truth or demonstrate unlawfully obtained gains shall be liable to seizure. The Supreme Court has determined that a mobile device can also be seized.[3]

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

Answer: The examining magistrate has a general competence to seize all objects that are prone to seizure (section 104 CPC). In other cases it depends on the nature of the offence. If the offence is mentioned in section 67 (1) CPC (offences which carry a statutory term of imprisonment of at least four years and certain other offences specifically mentioned) all investigating officers (police officers, public prosecutors, etc.) have a competence to seize the object (section 96 (1) CPC). There must be a reasonable suspicion that an offence has been committed, a known suspect is not required. Investigating officers also have the competence to seize objects carried by an arrested suspect (section 95 (1) CPC).

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

Answer: Yes. In order to reveal the truth seized objects can be investigated in order to obtain information that is relevant for the investigation. Data that has been saved on computers is not excluded.[4]

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?*

[3] ECLI:NL:HR:2017:584.
[4] ECLI:NL:HR:1994:AD2076.

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

Answer: Yes, there are limits but those are not (yet) explicitly defined by law. For now the Supreme Court has determined that an investigating officer who seized a smartphone is also allowed to search the phone. He has this competence based on the same legal provision as his competence to seize the phone (art. 94 Sv jo. art 95 and 96 Sv). The main question however is the extent of the intrusion of private life that is made with the search. If the invasion of privacy is limited, the general competence is considered a sufficient legal basis. If the infringement however is more than limited, a more specific legal provision is required. According to the Supreme Court an infringement is limited in case the investigation only consists of consulting a small number of certain data stored or available on the electronic data carrier or in the automated work. If that investigation is such that it provides a more or less complete picture of certain aspects of the personal life of the user of the data carrier or the automated work, that investigation by a police officer may be unlawful towards him. This may in particular be the case when it concerns the examination of all data stored or available in the electronic data carrier or the automated work using technical aides.[5]

In those cases the investigation can be conducted or ordered by the public prosecutor (section 96 CPC) or the examining magistrate (section 104) CPC. The Supreme Court ruled that '[i]n such a case, the aforementioned legal provisions provide an adequate basis for investigating seized objects - including electronic data carriers and automated works - that involve a more than limited intrusion into privacy. In the light of art. 8 ECHR an investigation by the examining magistrate can be considered in particular in cases where it can be predicted in advance that the invasion of privacy will be very drastic.[6]

In the proposal for a new CPC section 2.7.4.1.1 stipulates that the public prosecutor can order an investigation in a seized electronic data carrier or automated work.

[5] ECLI:NL:HR:2017:584.
[6] ECLI:NL:HR:2017:584.

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

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

Answer: Yes, if the owner of the device gives his consent the search is no longer considered a coercive measure and therefor the limitation mentioned do not apply.

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

Answer: According to section 125k CPC insofar as is specifically required in the interest of the investigation, the person who may be reasonably believed to have knowledge of the security system of a computerised device or system may be ordered, in case of a search, to provide access to the computerised devices or systems present or parts thereof. The person who is ordered to do so must comply with this order, if requested, by providing the knowledge about the security system. However, according to section 125k (3) CPC the order shall not be given to the suspect.

Since section 125k CPC only applies in case of a search, according to section 126nd CPC in the case of suspicion of a serious offence as defined in section 67(1), the public prosecutor may, in the interest of the investigation, request the person, who may be reasonably presumed to have access to specific stored or recorded data, to provide this data. This provision can include data necessary to unlock a device. However there is a special provision in section 126nh that says the public prosecutor may, if required in the interest of the investigation, in or immediately after the application of a.o. section 126nd, order the person who may be reasonably presumed to have knowledge of the manner of encryption of the data referred to in these sections to assist in decrypting the data by either undoing the encryption, or providing this knowledge.

None of these request can be given to the suspect (section 126nd (2), section 126nh (2) CPC). This means a suspect can not be requested to provide a code or password since that would be contrary to the right not to incriminate one-self enshrined in art. 6 ECHR.

However when the device is locked with a biometric lock, for example a face scan or fingerprint, the law enforcement agencies are allowed to hold the device in front of the owners face or to grab his finger and hold it on the device in order to unlock the device[7], because these materials exist independent of the will of the suspect.

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

Answer: If an object is seized the person in possession of the object at the moment of seizure will receive a proof of delivery if possible (section 94 (3) CPC). There is no obligation to inform the owner of the mobile device (if that person is not the same as the person in possession at the moment of seizure).

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

Answer: Yes. In order to reveal the truth seized objects can be investigated in order to obtain information that is relevant for the investigation. Data that has been saved on computers is not excluded. This also applies to electronic data carriers and computerised devices and system, including smartphones, stored or available data. There are no statutory limitations to the means used to conduct the investigation.

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

Answer: No.

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*

[7] ECLI:NL:RBNHO:2019:1568.

Investigation Order or Mutual Legal Assistance Treaties the only route or do other options exist? Please elaborate.

Answer: According to Section 126nf CPC in the case of suspicion of a serious offence as defined in section 67(1) CPC (offences which carry a statutory term of imprisonment of at least four years and certain other offences specifically mentioned), which serious offence in view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of law and order, the public prosecutor may, if urgently required in the interest of the investigation, request the person, who may be reasonably presumed to have access to data, to provide said data. This request may only be made following prior written authorisation to be granted by the examining magistrate on application of the public prosecutor.

If it is known that the data resides outside the jurisdiction such a request can only made via an EIO of MLAT. However, e.g. Microsoft retains a Dutch law firm that handles requests pertaining to Hotmail-data. The company tends to voluntarily comply with the request. Therefor a MLAT is no longer needed.

26. *What about data stored in the Cloud, where you are unable to determine the location of the server or the identity of the service provider?*

Answer: This situation is not provided for under Dutch law at the moment. The request based on Section 126nf CPC (see above) assumes that the identity of the service provider is known. In that case the request can be made and the service provider is obliged to comply. According to Section 125j CPC *in the case of a search*, a computerised device or system located elsewhere may be searched for data stored in that device or system that is reasonably required in order to reveal the truth from the place where the search takes place. Should it be known at the time of the search that the data accessed resides outside the jurisdiction, an EIO or MLAT would be the correct route. However, should data stored in the Cloud in another jurisdiction be used in proceedings, a complaint that that procedural requirements were not complied with will not lead to any consequences because the Supreme Court ruled that a suspect cannot complain about infringements made on the sovereignty of another State.

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

The current CPC has no provision for accessing data stored on a computerised device or system located elsewhere *in case of seizure* of a mobile device.

In the proposal for a new CPC section 2.7.4.1.2 stipulates that the public prosecutor can order an investigation in a computerised device or system located elsewhere in case of 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?*

Answer: No, see the answer above. This would only be possible with a request based on Section 126nf CPC.

28. *How is the access to data kept by a Service Provider related to the device regulated? Is it performed upon a Court order, or also through other means?*

Answer: This depends on the type of data. Under Section 126na CPC in the case of suspicion of a serious offence, the investigating officer may, in the interest of the investigation, request the provision of data pertaining to name, address, postal code, town, number and type of service of a user of a communication service (in other words: administrative data).

Under Section 126n CPC in the case of suspicion of a serious offence as defined in section 67(1), the public prosecutor may, in the interest of the investigation, request the provision of data on a user of a communication service and the communication traffic data pertaining to that user (in other words: communication data). Under Section 126nd CPC in the case of suspicion of a serious offence as defined in section 67(1), the public prosecutor may, in the interest of the investigation, request the person, who may be reasonably presumed to have access to specific stored or recorded data, to provide this data (in other words: all data the service provider keeps pertaining to the services rendered to the user of the device other than administrative data or communication data). Under Section 126nf CPC in the case of suspicion of a serious offence as defined in section 67(1) CPC (offences which carry a statutory term of imprisonment of at least four years and certain other offences specifically mentioned), which serious offence in

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

view of its nature or the relation to other serious offences committed by the suspect constitutes a serious breach of law and order, the public prosecutor may, if urgently required in the interest of the investigation, request the person, who may be reasonably presumed to have access to data, to provide said data. This request may only be made following prior written authorisation to be granted by the examining magistrate on application of the public prosecutor. This provision pertains to data stored by the service provider that is not communication between the service provider and the client (e.g. e-mail, voicemail,, etc.).

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

Answer: See the answer above. The more serious the invasion of privacy, more guarantees are provided for.

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. 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: According to Section 359a CPC the Court may, if it appears that procedural requirements were not complied with during the preliminary investigation which can no longer be remedied and the law does not provide for the legal consequences thereof, determine that:
a. the length of the sentence shall be reduced in proportion to the gravity of the non-compliance with procedural requirements, if the harm or prejudice caused can be compensated in this manner;
b. the results obtained from the investigation, in which there was a failure to comply with procedural requirements, may not be used as evidence of the offence as charged in the indictment;
c. there is a bar to the prosecution, if as a result of the procedural error or omission there cannot be said to be a trial of the case which meets the principles of due process.
In the application of a remedy the Court shall take into account the interest served by the violated rule, the gravity of the procedural error or omission and the harm or prejudice caused as a result of said error or omission.

According to the case-law of the Supreme Court remedies can only be applied in case the infringement on procedural requirements took place in the preliminary investigation leading to the prosecution of the suspect. E.g. in the case of a search without meeting the procedural requirements that led to the prosecution of a suspect that had threatened the police officers conducting the search, the Supreme Court ruled that the search had not taken place in the preliminary investigation that lead to the prosecution for threatening the police officers.[8]

Furthermore, remedies can only be applied in case the infringement on procedural requirements harmed the suspect. E.g. If procedural requirements were not complied with during the search of a mobile device of a third person leading to evidence in the case of the suspect, the suspect cannot claim his rights were infringed.

[8] ECLI:NL:HR:2005:AU3297

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

According to the case-law of the Supreme Court exclusion of evidence is only possible if the irregularities occurred in the investigation leading to the prosecution of a suspect, when the irregularities breached the suspects rights and when the use of evidence obtained as a result of unlawful actions by investigating officers would result in a breach of the right to a fair trial.[9]

E.g. if a suspect is questioned without prior access to a lawyer, the statement of the suspect cannot be used as evidence since that would lead to a breach of the right to a fair trial.

The Supreme Court ruled that exclusion of evidence is only possible if the evidence has been obtained through the omission and only qualifies if the unlawful gathering of evidence has significantly violated an important provision or legal principle.

The Supreme Court emphasizes in this regard that a violation of the provisions that guarantee the right to respect for privacy (art. 8 ECHR) does not automatically constitute an infringement of the right to a fair trial.[10]

Under the current case-law of the Supreme Court it is hard to think of any situation in which not following the applicable rules leads to inadmissibility of the evidence unless not following the applicable rules could lead to flaws in the reliability of the evidence.

In all other cases, the Court should take into account the interest served by the violated rule, the gravity of the procedural error or omission and the harm or prejudice caused as a result of said error or omission.

[9] ECLI:NL:HR:2004:AM2533 and ECLI:NL:HR:2013:BY5321.
[10] ECLI:NL:HR:2009:BH8889

For that matter, it does not make a difference whether a mobile device was seized or not.

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: We have not found any published protocols or case-law referring to protocols. It is known that Dutch investigating officers work with the Forensic Toolkit software made by AccessData. Typically an image will be made of a seized data carriers or automated work in order to guarantee the reliability of the investigation.

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.

31. **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: Issues would arise at the moment gathering information that is available in another jurisdiction would be necessary. See the answer to question 19. In the vast majority of cases in which a mobile device is seized, data accessible in that device can be investigated after an order by a public prosecutor. In those cases the forensic examiner will have knowledge of the nature of the crime in order to know what to look for. In those cases knowledge of the regional laws/legislative framework of other jurisdiction is not needed.

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

In cases where information of service providers in other jurisdiction is necessary, the public prosecutor will ask the MLAT-office at the Ministry of Justice and Security to assist.

32. **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: Section 5.1.1 through 5.5.13 CPC provide for incoming and outgoing MLAT's and European cooperation in criminal matters (such as the EIO (Sections 5.4.1-5.4.31). In these provisions the procedure to the EIO or another instrument for cross-border gathering of evidence within the EU is laid down. There is no established procedure describing how to decide to use these international instruments.

33. **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: In practice the EIO is used in cases where it can be used, using the appendices to the Directive

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

Answer: As far as we know there is no cooperation with the private sector in conducting forensic investigations. Regular digital forensic investigations are being conducted by specifically trained digital forensic investigators. The more difficult investigations can be conducted by the Dutch Forensic Institute of the Ministry of Justice and Safety (www.forensicinstitute.nl)

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

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

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

- *Data protection concerns (Law Enforcement Directive 2016/680 and implementing national law)*
- *Privacy concerns and respect for core area of private life (i.e. how is it guaranteed that very sensitive information, not relevant to the investigation is not used)*
- *Human rights such as the right to a fair trial (tools may deliver faulty results and methods used are often untransparent) and the right to non-discrimination (tools that are untransparent may contain bias)*
- *What information can be retained/copied? For how long?*

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

Answer: There are no rules on how the data must be analysed. Of course there are rules pertaining to the retention of data.

The Police Data Act (Wet politiegegevens) pertains to all data collected by the police in the course of police activities, such as criminal investigations. The Police Data Act lays down rules pertaining to the processing and retention of data. The Judicial and Criminal Data Act (Wet justitiële en strafvorderlijke gegevens) pertains to data processed and retained by the public prosecution service. Both acts stipulate that data can only be retained if this is necessary to achieve the goals described in these acts (the execution of the police task and the proper administration of criminal justice).

According to the Police Data Act data should be destroyed when retention is no longer necessary to achieve the goals served by processing the data. The police data will be destroyed as soon as they are no longer necessary for the execution of the daily police task and will in any case be deleted no later than five years after the date of the first processing (Section 8 Police Data Act).

According to Section 9 Police Data Act Police data can be processed specifically for the purpose of an investigation with a view to maintaining the rule of law in a specific case and should be destroyed when retention is no longer necessary for the goal of the investigation.

According to the Judicial and Criminal Data Act judicial data pertaining to suspects and convicted persons will be destroyed within a. 30 years after the final decision on the case when the case pertained to a serious offence (offences which carry a statutory term of imprisonment of at least six years) of 20 years after the death of the person involved, b. 20 years after the final decision on the case when the case pertained to a less serious offence and c. after the limitation period bars prosecution. These terms will be prolonged if a persons is convicted to a term of imprisonment of more than 20 years and in cases pertaining to sexual offences.

Under both laws the data subject has the right to request the correction, destruction or blocking of the processing of personal data concerning him.

Furthermore, the police and prosecution are bound by the proportionality principle which means that data which are not relevant to the investigation should be destroyed.

In practice, destruction of data does not seem to be considered very important by the police.

Section 3: Admissibility of evidence before court

36. **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.

37. **Question:** *Are the criteria for admissibility of evidence collected through mobile forensics the same as for the other types evidence? Please elaborate in any case.*

Answer: Yes, there are no special criteria for evidence collected through mobile forensics.

38. **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: Yes, it depends on the severity of the breach and the extent to which the defendant has been harmed in his defense. The rules mentioned in answer 30 are applicable.

39. **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: No. The Supreme Court ruled that, in principle, the suspect has no legally respectable interest in the observance of international law by Dutch investigating officers abroad.[11]

40. **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: In general a forensic image will be made of the seized mobile device in order to ensure that the results of the forensic investigation remain reliable. The only reason to render the evidence inadmissible would be if there is doubt regarding the reliability of the evidence.

41. **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.*

[11] ECLI:NL:HR:2012:BV9070.

Answer: No.

***42.* 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: In the following case the defense argued that the evidence obtained by investigating the smartphone of the defendant was inadmissible. The investigating officers had seized and searched the phone on the basis of art. 94 jo. 95 and 96 Sv. During this investigation they used software to circumvent the security and copied the all data that was saved on the phone. Later the investigators searched the copied data. The police stated that they did not search all data, but that they were selective. However they never elaborated on the criteria used to determine what data was worth investigating. The Supreme Court determined that is was a procedural mistake that cannot be fixed and thus lead to a breach of art. 8 ECHR. This could however not lead to exclusion of evidence like the defense argued. A mere observation that a procedural mistake was made was sufficient.[12]

***43.* Question:** *Is there in your jurisdiction an established and recognised standardisation(s) of the processes of collection, analysis, interpretation and reporting of digital evidence that must be followed for the evidence to be admissible? (as critical to the validity of evidence, their quality and impact evidence's acceptance by the courts)? If yes, please elaborate.*

Answer: No.

***44.* 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: No. The Data Protection law states that personal data with a criminal nature can be processed by bodies that deal with the application of criminal law. Furthermore, see the answer to question 30.

[12] ECLI:NL:HR:2019:1079

***45.* 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: In multiple cases the defense questioned the admissibility of evidence obtained during the investigation in a smartphone because a procedural mistake was made. There are however no cases were the judge ruled that any consequences must follow from such a procedural mistake. If the court came to the conclusion that a mistake was made, the observation of this mistake was sufficient.[13]

[13] ECLI:NL:HR:2018:1121, ECLI:NL:HR:2018:2323, ECLI:NL:HR:2019:1079.

Section 4: Interpretation and presentation of evidence from mobile forensics before the Court

46. **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: No. Two things are important in this respect.

The judge judging the facts is free to select and evaluate the available evidence and to use in evidence the material he deems reliable. However, that provision does mean that he will have to give further reasons for his decision in a number of cases. There are no general rules regarding the cases and the extent to which a decision must be reasoned in more detail, due to the many, diverse situations that may arise. In that context, significance will be attributed, inter alia, to the nature of the subject raised, as well as the content and intrusiveness of the arguments put forward.[14]
Therefore, different types of evidence are not measured to their probative value. This is up to the judge to decide. This also means there are no rules on how to interpret evidence.

The instruction technical criminal investigation / expert investigation, drafted for the purpose of the public prosecution/investigating officers to decide whether an expert should be consulted,

[14] ECLI:NL:HR:2006:AU9130.

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

regular forensic investigation into mobile devices does not require a registered expert, but can be conducted by investigating officers. It is therefore not common practice that the evidence is examined by a (independent) expert witness.

47. **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.

48. **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.

49. **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. There are many cases in which the legality of the investigation of a mobile device was questioned (because the investigation would lead to an invasion of privacy (see the answer to question 45), but no cases in which the reliability of evidence collected through mobile forensics was questioned pertaining to mobile devices.

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

50. **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: The Supreme Court has determined that an investigating officer who seized a smartphone is also allowed to search the phone. He has this competence based on the same legal provision as his competence to seize the phone (art. 94 Sv jo. art 95 and 96 Sv). The main question however is the extent of the intrusion of private life that is made with the search. If the invasion of privacy is limited, the general competence is considered a sufficient legal basis. If the infringement however is more than limited, a more specific legal provision is required. According to the Supreme Court an infringement is limited in case the investigation only consists of consulting a small number of certain data stored or available on the electronic data carrier or in the automated work. If that investigation is such that it provides a more or less complete picture of certain aspects of the personal life of the user of the data carrier or the automated work, that investigation by a police officer may be unlawful towards him. This may in particular be the case when it concerns the examination of all data stored or available in the electronic data carrier or the automated work using technical aides.[15]

In those cases the investigation can be conducted or ordered by the public prosecutor (section 96 CPC) or the examining magistrate (section 104) CPC. The Supreme Court ruled that '[i]n such a case, the aforementioned legal provisions provide an adequate basis for investigating seized objects - including electronic data carriers and automated works - that involve a more than limited intrusion into privacy. In the light of art. 8 ECHR an investigation by the examining magistrate can be considered in particular in cases where it can be predicted in advance that the invasion of privacy will be very drastic.[16]

[15] ECLI:NL:HR:2017:584.
[16] ECLI:NL:HR:2017:584.

The results of an investigation will be part of the case-file as far as these results may be of importance for any decision the judge should make. According to Section 34 CPC the suspect may request the public prosecutor to add to the case documents specifically described documents that he considers relevant for the assessment of the case.

***51.* 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.

***52.* 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.

***53.* 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: The prosecution is responsible for the police investigation, the decision to prosecute and the decision which offenses will be prosecuted and the indictment.

The Court shall, on the basis of the indictment and the hearing at the court session, deliberate on the question whether it has been proven that the defendant committed the criminal offence, and, if so, which criminal offence the judicial finding of fact constitutes under the law; if it is found that the offence is proven and punishable, then the District Court shall deliberate on the criminal liability of the defendant and on the imposition of the punishment or measure, prescribed by law. According to section 315 CPC if the Court finds that the questioning at the court session of witnesses, who have not yet been questioned, or the submission of documents or convincing items of evidence, which are not yet available at the court session, is necessary, it shall order that, if

necessary with an attached order to forcibly bring them, these witnesses be summoned or called in writing to appear at the court session at a date and time to be set by it or that these documents or convincing items of evidence be submitted.

The defendant can call witnesses or experts, request the public prosecutor or the Court to add to the case documents specifically described documents that he considers relevant for the assessment of the case and can ask for a counter-investigation. Eventually the judge will decide whether hearing witnesses or experts is in the interest of the defence or necessary for the Court's decision and whether adding documents or counter-investigation is necessary.

Witnesses have no procedural rights. They are obliged to appear and answer truthfully.

Victims have a right to have access to the part of the case documents that are in their interest and have a right to give a statement in cases that involve crimes of violence and sexual offences.

5.1 The Prosecution

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

Answer: Not that we know of. Perhaps there are internal guidelines.

5.2 The Court

***55.* 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.

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

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

Answer: The results of investigation into mobile devices will be laid down in a report drafted by the investigating officer. The report is dated and signed under the oath of office. The Courts tend to view the oath of office of a police officer as an important guarantee for the correctness and reliability of the contents of the report.

In a report containing evidence obtained via mobile forensics typically the entire process of investigating the mobile device will be explained (from the moment the investigating officer received the mobile device, the techniques used, to the evidence obtained).

In case the Court would consider itself to be insufficiently informed (for example in response to remarks made by the defendant) the investigating officer can be asked to draft an additional report, be summoned as a witness or an expert could be appointed.

5.3 The defendant and defender

***57.* 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: According to Section 30 CPC the suspect has a right to receive copy of the case documents containing the police reports in which the investigation leading to the acquired mobile evidence is laid down. In general, the tools used, the procedures used, the parties involved and how the validity of the results is guaranteed will be laid down in the police report. In case the defense can show reasons to doubt if the methods used to acquire mobile evidence produce reliable evidence a request could be made to appoint an expert to elaborate on the software and methods used to acquire evidence.

We are not aware of any cases in which the defense asked for a copy of the image that was made of a mobile device in order to investigate the data by the defense.

5.4 Witnesses

58. **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: Statements of anonymous witnesses can only be used in evidence in corroboration with other evidence. The use of anonymous statements is therefore not too common. There is a special arrangement for 'threatened witnesses' (Section 226a CPC) who will be questioned by the examining magistrate. The examining magistrate will know the identity of the witness and will draft a report pertaining to the reliability of the threatened witness. The suspect and his counsel can pose questions to the threatened witness but cannot be present during questioning. Answers to questions that can lead to the identity of the witness will be barred.

During police investigation a witness can choose domicile, in order to prevent his personal address will be named in the case documents.

There are no other rules to preserve the privacy of witnesses and there are no particular requirements for witnesses regarding their capability to testify in terms of mobile forensics.

5.5 The Victim

59. **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.*

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

Answer: Victims in criminal cases have a right to a copy of the case documents that are relevant to them under section 51b CPC. The victim may request the public prosecutor to add to the case file documents that he considers relevant for the assessment of the case against the suspect or his claim against the suspect. Victims can claim damages and can give a victim statement in cases concerning violent crimes and sexual offences.
Under Section 269 CPC the Court may order that the entire hearing or part of the hearing be held behind closed doors. This order may be given in the interest of public decency, public order, state security, and if required in the best interests of minors, or in the interest of respect for the personal life of the defendant, other participants in the criminal proceedings or persons otherwise involved in the case.

In cases concerning sexual offences against minors the decision was made not to mention the names of the victims but to suffice with a character (A, B, C, etc.).

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: The Dutch criminal procedure is mainly a written procedure, meaning that witnesses are being questioned by police-officers and their statement will be laid down in a police-report. On request by the defense witnesses can be questioned by an examining magistrate but it is fairly rare that witnesses are questioned during trial. The same applies to experts.

This also mean that evidence acquired using mobile forensics will reach the judge in a written report in which the software and methods used will be described. Dutch Courts tend to value written reports and only in cases where a substantiated claim is made that the results of an investigation or not reliable, the judge will consider an investigation into the reliability of the results.

E.g. in a big investigation into organized crime murders the servers of the Canadian company Ennetcom were seized. Ennetcom offered PGP (Pretty Good Privacy)-telecommunications. All messages send via these PGP-telephones were retained on the server.

In order to search the server the Dutch Forensic Institute developed a search tool named Hansken. In several cases defense asked questions about the reliability of the results of this research tool (were only incriminating messages found or were all messages found and how can defense exercise its rights?), leading the Court to appoint an expert to answer questions concerning the server and the search tool.