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: Member of the judiciary.

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

Answer: Germany.

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: Not specifically for purposes of criminal law or criminal procedure. In telecommunications law a communications terminal („Telekommunikationsendeinrichtung") is defined as

> *eine direkt oder indirekt an die Schnittstelle eines öffentlichen Telekommunikationsnetzes angeschlossene Einrichtung zum Aussenden, Verarbeiten oder Empfangen von Nachrichten; sowohl bei direkten als auch bei indirekten Anschlüssen kann die Verbindung über elektrisch leitenden Draht, über optische Faser oder elektromagnetisch hergestellt werden; bei einem indirekten Anschluss ist zwischen der Telekommunikationsendeinrichtung und der Schnittstelle des öffentlichen Netzes ein Gerät geschaltet (§ 3 Nr. 24a Telekommunikationsgesetz).*
>
> *https://www.gesetze-im-internet.de/tkg_2004/__3.html*

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?*

Only if the legitimate user of the device consents.

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?*

There are no explicit limits in statutory law on using data gathered by such searches as such searches aren't covered in German statutory law in the first place. To the contrary, the Code on Criminal Procedure (Strafprozessordnung, StPO) makes it clear that German law expects law enforcement to properly seize any "papers" or media they want to sieve through, see § 98 StPO and § 110, subsection 3 StPO.

Note: An official translation of the German code of Criminal Procedure (Strafprozessordnung, StPO) provided by the Federal Department of Justice is accessible at

https://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html

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

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

See answer to question 5.

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

See answer to question 5.

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

See answer to questions 4 and 5.

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

No, if they are suspects / defendants in the investigation, as this would be considered forced self-incrimination in breach of the principle *nemo tenetur se ipsum accusare* which, under German constitutional law, is protected as an aspect of the rule of law, see Article 20, subsection 4 of the German constitution (Grundgesetz, GG). This principle is also protected by § 136a StPO.

Witnesses, however, are legally required to unveil passwords. If they refuse, they may be incarcerated by court order for up to six months to force them to comply. See § 70, subsection 2 StPO:

> *(2) Detention may also be ordered to force a witness to testify; such detention shall not, however, extend beyond the termination of those particular proceedings, nor beyond a period of six months.*

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

See answer to question 5.

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

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

A formal search requires the device to be seized; please see section on seized devices below.

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

A formal search requires the device to be seized; please see section on seized devices below.

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.*

Accessing data in the Cloud is regulated by § 110, subsection 3 StPO. Technically this provision only concerns cloud access during searches of premises and does not contain any explicit limitation to data physically stored in Germany. Legal doctrine assumes, however, that the Convention on Cybercrime is applicable in these instances, limiting the right to access data stored outside of Germany. See the discussion in the answer to question 41 for details.

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

A formal search requires the device to be seized; please see section on seized devices below.

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.*

German criminal procedural law is very lenient as to the consequences of violations of criminal procedure during investigations. As a rule, violations of criminal procedure have no (!) consequences on the admissibility of evidence or on the persuasive value of evidence. They may nevertheless have disciplinary consequences for the offending officers, but that obviously doesn't help individuals subject to illegal investigatory practices. The basic reasoning behind this

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

longstanding case law is the assumption that German police officers just don't break the law, so there was no need to "punish" them in case of violations by considering evidence inadmissible.

§ 136a StPO contains very limited exceptions to this rule by defining situations that lead to inadmissible evidence. This section explicitly forbids to limit the suspect's ability to make up their mind and express their will by means of torture, exhaustion, bodily harm, application of substances, deception or hypnosis. Statements made under circumstances that violate these rules may not be used in court. However German case law tends to construe the aforementioned illegal circumstances very narrowly. For example, many ploys police officers may use during an investigation aren't considered "deceptions" but only "investigatory wit" (kriminalistische List), resulting in the evidence gathered being admissible as the "wit" applied is considered out of scope of § 136a StPO.

Mobile device seized

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

Yes, under § 94 and § 98 StPO. Please see the detailed answer to question 37 for issues around seizure.

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

Please see the detailed answer to question 37.

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

Yes; under § 110 StPO.

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?*

Please see the detailed answer to question 37.

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?*

If the person in possession of an object consents to the object being taken into custody, no formal seizure is necessary. See § 94, subsection 2 StPO.

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

No, provided they are also suspect / defendant to the investigation. See answer to question 9 for details.

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

The person is usually aware of the object being taken into custody as the person needs to consent (see § 94, subsection 2 StPO) lest a formal seizure is required, of which the person will be notified.

Other than that, there is no formal requirement to notify the person of the authorities' intent to analyze seized devices.

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

Yes, there are no limits on using techniques to "crack" encrypted / locked evidence provided that no suspect / defendant is forced to self-incriminate.

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

See answer to questions 9 and 23.

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

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.*

There is no German statutory law on this matter, however doctrine applies Art. 31 and 32 of the Convention on Cybercrime. See answer to question 41 for details.

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?*

See answer to question 41 for details.

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?*

Yes, provided that the Cloud storage is accessible from the seized device; see § 110, subsection 3 StPO.

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?*

Data about past telecommunications may be requested from the provider issuing the SIM card used in the device under § 100g StPO. Such requests usually require a court order unless in cases of extreme urgency where a prosecutor may authorize such requests.

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

No.

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

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.*

No, usually not. The only instance where data may be inadmissible that comes to mind is if

- a suspect was not informed about their right to remain silent – an omission in breach of § 136 StPO,
- the suspect later "voluntarily" gives up a password under the false assumption to be required to give up the password,
- data is accessed using this password that wouldn't have been accessible otherwise.

I have only been able to identify a single case where such a situation was in question. The Berlin-Tiergarten magistrate court (Amtsgericht Tiergarten 353 Gs 241 Js 2317/17; January 25, 2018) held that if a suspect was not informed about the right to remain silent, the password produced may not be used to unlock an iPhone and acquire data using this password (StraFo 2018, 67). The court didn't decide, however, if data would have been admissible in court if the password had already been used and the iPhone copied.

I assume that such data would be admitted in court as German courts traditionally reject the "fruit of the poisonous tree" doctrine.

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.

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

Answer: Indication of length of answer: at least a couple of pages, as this is the main overview question.

31.* Question: In cases where the examination or data acquisition is not possible without changing the configuration of the device, is there a strict protocol that should be followed (e.g. procedure and changes should be tested, validated, and documented)? If yes, please specify on what rules this is based and what the requirements are. Please also provide examples.*

Answer: No, there is no such protocol that I know of.

***32.* Question:** *Are there any specific rules in criminal procedure that regulate the use of mobile forensics tools using/deploying AI technology? Are there any conditions which need to be met so AI-powered tools could be applied in the process of evidence collection?*

Answer: No.

***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: Criminal law and Criminal procedural law is almost entirely federal law in Germany so such issues usually don't arise.

***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?*

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

Answer: Not that I know of, but I haven't worked as a prosecutor so far so this question may be beyond my expertise.

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: See answer to question 34.

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

Answer: No, but see answer to question 34.

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

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

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

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

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

Answer: As a rule, German statutory law lacks specific provisions as to the use of digital information in criminal proceeding. The acquisition, analysis and later use of data from seized devices is regulated by laws that originally had in mind the search of premises and seizure of papers. Therefore, only general principles can be directly derived from statutory law. In front of this backdrop it may at first strike as surprising that case law on these issues is very scarce as well. This becomes more understandable bearing in mind that violation of procedural rules almost never leads to issues of admissibility of evidence in court proceedings. For this reason, defendants usually have little motivation to question the gathering of evidence: Once it's there, it can be used against them – even though it may have been acquired in questionable ways. See the answer to question 15 for rare exceptions to this rule.

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

That said, under German law three logical steps need to be clearly distinguished when working with physical or digital evidence:

- **Acquisition** of objects by law enforcement ("Sicherstellung")
- Formal **seizure** ("Beschlagnahme")
- **Analysis** of acquired objects, including papers and digital information.

§ 94, subsection 1 StPO holds that objects that may be relevant to an inquiry as evidence are to be **acquired**.

Under § 94, subsection 2 StPO a formal **seizure** is necessary if objects aren't relinquished voluntarily. In practice this becomes most relevant to evidence that is acquired during a search when the prior holder of the evidence protests against the acquisition.

Finally, § 110 subsection 1 StPO allows prosecutors to "**sieve through papers**" that have been seized. Prosecutors can delegate this authority to police officers. Without such authorization, police officers require consent of the person who had such papers in their possession (§ 110 subsection 2 StPO). The provision is generally understood to apply to all means of storing information, including digital storage media (BVerfG 2 BvR 2248/00, January 30, 2002).

Protections in light of **privacy concerns** or **professional secrets** apply at various stages of these three steps:

Under § 97, subsection 1 StPO seizure does not extend to certain papers that are covered by professional or personal secrecy. For example, written messages between a suspect and his relatives (see § 52 StPO) or certain professionals like defense attorneys or priests (see § 53, subsection 1, numbers 1 to 3b StPO) may not be seized unless they were acquired out of the possession of the suspect or third parties.

Protections for the **core area of private life** have not yet been introduced into this field of German law. So far, the Federal Constitutional Court has demanded such protections only in instances of secret / undercover acquisition of data, e.g. by wiretapping (§ 100a StPO). However, courts have

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

demanded that during the acquisition stage as well as the analysis stage the principle of proportionality be respected: Law enforcement may only acquire objects and information that may reasonably be considered relevant for the inquiry, and data that seems to be of only private nature may not be analyzed. It must be underlined that such protections are rather weak as it is virtually impossible to enforce these rules in practice: Police officers analyze seized information without third party supervision, so they could sieve through a suspect's home-made porn videos if they are so inclined without anyone even noticing.

Section 3: Admissibility of evidence before court

38. **Question:** *Are there general rules or guidelines on the admissibility of electronic evidence in your jurisdiction applicable to mobile forensics, not yet discussed above?*

Answer: There are no specific rules of admissibility for digital evidence.

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: The criteria are indeed identical.

German law knows very few limits on admissibility for any type of evidence; the most notable exceptions have been discussed in answer 15.

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?*

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

Answer: As a rule, whatever law enforcement is able to assemble during an investigation may be used in court, even if rules for collecting evidence have been violated. See the answer to question 15 for exceptions to this rule.

***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: Concerning the acquisition stage, this situation is addressed by § 110, subsection 3 StPO: When sieving through any means of data storage, law enforcement may also access (and copy data from) "remote data storage media" accessible from the first data storage. Technically this law doesn't limit remote access to media or devices physically located in Germany, and I am not aware of any case law addressing this situation.

Legal doctrine (e.g. Burhoff, Handbuch für das strafrechtliche Ermittlungsverfahren, Rn. 1742), however, cites Artt. 31, 32 of the Convention on Cybercrime (https://www.coe.int/en/web/conventions/full-list/-/conventions/ treaty/185). Under Art. 32 of said convention a

> *[…] Party may, without the authorisation of another Party:*
>
> *access publicly available (open source) stored computer data, regardless of where the data is located geographically; or*
>
> *access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.*

In other situations, as per Art. 31 of the Cybercrime Convention, German law enforcement is required to request mutual legal assistance. If these requirements aren't met, it is safe to assume that trial courts will not see any adverse consequences for the admissibility of the data acquired,

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

unless maybe in exceptional cases where law enforcement frivolously accesses data obviously stored abroad.

***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: German criminal procedure contains hardly any rules as to the way judges have to evaluate and balance evidence that was introduced into criminal proceedings. To the contrary, as per § 261 StPO judges are explicitly free to assess the evidence. In practical terms courts would probably hear one or more law enforcement personnel as expert witnesses to clarify the way the data was gathered, handled and possibly altered during the investigation.

***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: None of the above. Courts may still deem it necessary to hear expert witnesses as to professional best practices to gather and handle data. Usually, though, courts will hear law enforcement officials as expert witnesses who may tend to find their own / their colleagues' practices to meet professional standards.

Also bear in mind that given rather deficient remuneration in German public service, law enforcement is facing systematic issues hiring highly qualified IT professionals. In many instances these officials will be ordinary police officers with an interest in IT but without formal qualifications who have been more or less trained "on the job".

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

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

Answer: No.

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

Answer: Not to my knowledge.

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: 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: Not to my knowledge.

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

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

48. **Question:** *Are there general rules or guidelines on the interpretation and presentation of evidence from mobile forensics, such as:*

- *Is mobile forensic evidence given a certain probative value?*
- *Are there rules on how to interpret mobile forensic evidence or requirements which must be complied with for the evidence to be considered reliable?*
- *Must such evidence be examined by an expert witness?*
- *If not obligatory, is this a common practice?*
- *What are the requirements for experts (experience, independence, training, etc.)?*
- *Is there a centralised management of mobile forensic operations in your jurisdiction to ensure the work is compliant with standards and can be presented in court in a consistent manner?*

Answer: As per § 261 StPO, the court is free to assess the evidence:

> ***Principle of judge's free evaluation of evidence***
>
> *The court shall decide on the result of the taking of evidence at its discretion and conviction based on the entire content of the hearing.*

I am not aware of any further written rules pertaining to the assessment of digital evidence.

In practice courts would usually rely on expert witness statements in order to clarify the reliability and persuasiveness of digital evidence. Note that such an expert witness statement is not formally required by law. Nevertheless, any party to the trial can request that an expert witness be heard, and the court can only decline such a request under certain limited conditions (see § 244, subsections 3 and 4 StPO for details). As far as expert witnesses are concerned, it is of note that the court can deny a request to take evidence based on its own expertise:

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

> *Except as otherwise provided, an application to take evidence by examining an expert may also be rejected if the court itself possesses the necessary specialist knowledge. The hearing of another expert may even be refused if the opposite of the alleged fact has already been proved by the first expert opinion; this rule shall not apply to cases where the professional competence of the first expert is in doubt, if his opinion is based on incorrect factual suppositions, if the opinion contains contradictions or if the new expert has means of research at his disposal which seem to be superior to the ones of an earlier expert. (§ 244, subsection 4 StPO).*

For this reason, there has been considerable debate on the idea of having specialized chambers at district courts dealing with cases involving IT evidence in order to save time and money on expert witnesses. But to this day and to my knowledge no such chambers have been established.

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

Answer: No.

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: I am not aware of any such standard. Topics that are discussed as “chain of evidence” issues e.g. in U.S. law are usually brushed away quoting § 261 StPO – judges are free to evaluate,

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

which in turn is generally regarded sufficient in order to assure that evidence has not been tampered with. The general assumption is that

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

Answer: I have been unable to find any such case law.

The reason for this scarcity of case law is probably peculiarities of German criminal procedure law. A judgement by a district court in criminal proceedings can only be questioned in a procedure called *"Revision"*, a strictly limited review taking into account only violations of procedure (see §§ 337 ff . StPO for details). Furthermore, such errors can only be proven by (a) the text of the judgement or (b) the transcript of the court proceedings, which in turn only contains very limited details, e.g. there is now record whatsoever of the content of a witness statement other than the personal notes that judges or parties take during the audience.

Therefore, for legal and practical reasons, a judgement can't be attacked claiming that the facts on which the judgement is based were incorrect. The party willing to question a judgement is even barred from claiming that witness statements had been wrongly quoted. For purposes of review in the *Revision* stage, the facts are to be taken as stated by the district court, unless some violation of procedure as to how evidence is gathered can be established.

Thus, the only viable avenue to question a judgement pertains to errors in applying procedural law, e.g. by wrongly rejecting requests to take evidence. In light of this, experienced courts usually follow requests to take evidence if ever possible so as not to violate procedural law when rejecting the request, knowing that their decision will stand even if they don't mention the evidence or the witness statement in their judgement.

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.

53. **Question:** *Is there any training required by law for the judges, prosecution, expert witnesses, lawyers involved in cases with evidence coming from mobile forensics?*

Answer: There is no *required* training for judges in Germany at all once they're on the bench. Yet various training academies for the judiciary exist, most notably the *Deutsche Richterakademie* that runs two training facilities in Wustrau and Trier, and both tend to pay certain attention to issues of digitization.

54. **Question:** *Is there a pre-determined time duration/limitation period required for the extraction of evidence from mobile devices, time for decoding, reviewing and analysing of the data, time for reporting that data in a form that prosecutors and others can use?*

Answer: Not specifically, but the general right to a speedy trial (as established by the European Court of Human Rights) applies to all stages of criminal proceedings, including the investigation by police and prosecutors.

Investigations requiring analysis of digital evidence are very often delayed by lack of staff at specialized police units as public service in Germany faces tough challenges when hiring qualified IT personnel.

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

***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: With regard to evidence, the most important right is **access to the file of the case**, which includes the written case file but also all evidence gathered during an investigation that remains in official custody. Before charges are brought, the file and the remaining evidence is handled by the prosecution or – at its orders – by the police. The defendant, in principle, has the right to have the file inspected by an attorney (§ 147, subsection 1 StPO), but the prosecution can refuse access until no more harm can be done to the purpose of the investigation (§ 147, subsection 2 StPO). Witnesses as such do not have any right to access the case file, regardless of the status of the case. Victims of certain crimes, however, can declare their wish to join the proceedings as private accessory prosecutors (§ 395 ff. StPO) while this declaration does only take effect once charges are brought and the court accepts the joinder.

As soon as charges have been brought, the court is in charge of administering the case file. This is typically the time when the defense first inspects the file. It is of note that defendants as such may not inspect the case file, an obvious hindrance to any meaningful defense. Victims admitted as private accessory prosecutors have the right to have the file inspected by an attorney.

Once a case reaches the trial stage, the parties to the case – prosecution, defendants as well as private accessory prosecutors – have various procedural rights at their disposal:

- entitled to be present at the main hearing, this applies to a private accessory prosecutor even if he is to be examined as a witness
- summoned to the main hearing
- challenge a judge (§ 24 and § 31StPO)
- challenge an expert witness (§ 74 StPO)
- ask questions (§ 240 subsection 2 StPO)
- object to orders made by the presiding judge (§ 238, subsection 2 StPO)
- object to questions (§ 242 StPO)

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

- apply for evidence to be taken (§ 244 StPO)
- make statements under certain conditions (§ 257 and § 258 StPO)

Once a judgement is rendered, all parties can request review by a higher court, but in case of judgements by a district court this review is limited to Revision as explained above (see answer 51). Private accessory prosecutors are further limited as they can't attack a judgement claiming that the sentence was inappropriate (§ 400 StPO).

5.1 The Prosecution

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

Answer: No.

5.2 The Court

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

Answer: As a rule, the investigation is carried out entirely by the prosecution. Judicial review only comes into play when certain particularly intrusive measures are to be taken. In the context of digital evidence, the most important case is the requirement to seek judicial approval for seizure of any acquired item as soon as the possessor objects to the acquisition, see § 98, subsections 1 und 2 StPO:

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

Section 98 – Procedure for seizure

(1) Seizure may be ordered only by the court and, in exigent circumstances, by the public prosecution office and its investigators (§ 152 of the Courts Constitution Act). Seizure pursuant to § 97 (5) sentence 2 on the premises of an editorial office, publishing house, printing works or broadcasting company may be ordered only by the court.

(2) An official who has seized an object without a court order is, as a rule, to apply for court confirmation within three days if neither the person concerned nor an adult relative was present at the time of seizure or if the person concerned and, if he was absent, an adult relative of that person expressly objected to the seizure. The person concerned may at any time apply for a court decision. The competence of the court shall be determined by § 162. The person concerned may also submit the application to the local court in whose district the seizure took place, which shall then forward the application to the competent court. The person concerned shall be instructed as to his rights.

Further instances that would require court orders include wiretaps (§ 100a subsection 1 sentence 1 StPO) or remote forensic searches of devices using hacking techniques (§ 100a subsection 1 sentences 2 and 3, § 100b StPO).

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: Under German procedural law there is no distinct assessment stage pertaining to any gathered evidence. The assessment is part of the trial stage and subject only to the principle of free evaluation of evidence under § 261 StPO.

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

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: As a rule, the defendant has no right to inspect files, but their defender has such rights under § 147, subsection 1 StPO.

> ***Section 147 - Right to inspect files, right of inspection; accused's right to information***
>
> *(1) Defense counsel shall be authorized to inspect those files which are available to the court or which would have to be submitted to the court if charges were preferred as well as to view items of evidence in official custody.*

Regarding digital evidence two scenarios need to be distinguished based on a rather formal notion of the term "file":

First, the digital evidence may have formally been made part of the file, e.g. by printing it or by adding digital media to the file. In this case, the right to inspect files extends to digital media. This inspection is usually facilitated by sending the file to the attorney's office for a few days. While it is clear that the defender has the right to make copies of the file's pages, it is still unclear if this right also includes the right to make copies of digital media, but in practice this is what defenders will usually do, provided they have the technical abilities.

Second, the evidence may not technically have been made part of the file, e.g. if a mobile device was only examined or it was copied to media that have not been made part of the file but are stored separately. In this case the defenders only have the right to "view items of evidence", which in practice means that such items aren't sent to them. Rather, the defender would need to go inspect the items at the prosecutor's office or a police station, see e.g. BGH

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

(Bundesgerichtshof, Federal Highest Court) 1 StR 355/13, February 11, 2013, concerning audio files of wiretaps: It is sufficient to give defense counsel access to the recordings at a police office. A few authors claim nevertheless that the right to a fair trial under Article 6 HRC may require that copies of digital evidence be made and sent to defenders if the inspection at police premises is insufficient for effective legal defense (see references in BGH, ibid., paragraph 24).

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: I am not aware of specific rules to this end. But the principle of proportionality also applies to the analysis of seized digital media: Only such information may be included in the file and used in court that is relevant to the inquiry.

In practice, however, such requirements are usually hard to implement as the defendant as their counsel have the right to inspect *all* evidence in official custody, not only such evidence that the prosecution deems relevant und not "too private". If, for example, a seized mobile device contained highly private imagery, it would still be legally impossible to prevent the defense from inspecting these files on the phone. On the other hand, the defense wouldn't be allowed to have such evidence introduced in court unless such images had any relevance to the investigation.

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.*

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

Answer: The victim is considered a witness, so the answer to question 60 applies to them as well.

Additionally, if victims have successfully applied to be admitted as private accessory prosecutors, they have the right to inspect the file of the case as well as the objects of evidence in official custody. See the answer to question 55 for details.

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: When working through the questionnaire I had the strong sentiment that quite a few underlying concepts / assumptions didn't quite "fit" to German criminal procedure and doctrine. I still tried to answer all questions to the best of my knowledge. Please feel free to follow up with specific questions if I missed the sense of a question.

Due to Corona quarantine regulations during the work on this questionnaire I have not been able to look up much case law but had to work primarily with the Code of Criminal Procedure and other sources that I could access online. Given the German civil law system that is not quite as problematic as it might be in a case law system. Nevertheless, please feel free to request case law backing statements of particular importance and I shall try my best to find such decisions.