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: Nora Katona – researcher at the Ludwig Boltzmann Institute of Fundamental and Human Rights

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

Answer: Vienna, Austria

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 legally defined term for 'mobile devices'. Within the legal system they are recognised as evidence as physical object which has a certain appearance, can carry traces etc. Secondly, the cell phone is a carrier of data. Data is information (see e.g. Art 4 Z 1 DSGVO [data protection order]), but in (material) criminal law also programs (see § 74 Abs 2 StGB [criminal code]). As immaterial objects, data require material embodiment on data carriers for their existence (see EBRV BlgNR 22. GP, 156). The cell phone is such a data carrier.

Technically, a further distinction can be made between data stored locally on the device and data that is only accessible through the device by (temporarily) creating a local copy. This applies, for example, to data that is (primarily) stored on a cloud server (see implicitly OGH 14 Os 51/18h).

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?*

Here two constellations are to be distinguished. First, the cell phone has been secured but not yet seized (confiscated). This is possible to secure evidence (§ 110 para.1 StPO). Secondly, the mobile device is not in the custody of the law enforcement authorities at all. If the cell phone is not in the custody of the law enforcement authorities, three possible types of access would be possible: 1) a program is installed on the cell phone of the person concerned, which can provide information about the data or use of the device; 2) information are accessed by the provider; 3) an object not belonging to the cell phone is installed, which could provide information about its data or use. These access possibilities can be summarized as "online searches" (see Heißl, Grundrechtskollisionen am Beispiel von Persönlichkeitsrechten sowie Überwachungen und Ermittlungen im Internet, 267f.).

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 specificities when it comes to information about data concerning messages (§ 135 para 2 StPO) that can be only requested by a court order. The information about data of a message

transmission comprises according to § 134 Z 2 StPO traffic, access and location data. Traffic data includes in particular the active and passive subscriber number as well as the time and duration of the connection and the amount of data transmitted. Access data are only covered by § 135 (2) to the extent that they are not concerning IP addresses as they are regulated in § 76 a para. 2 StPO. Location data indicates the geographical location of a communications service user, and the data that indicates the geographical location of a communications service user that occur during an upright communication, as well as those that solely by the fact that the device in question is ready for operation by being connected to the network of the respective communications service provider (Bauer, Verwertunsgverbot, p. 203).

Equally, there are specificities for the surveillance of messages and their transmission. For messages (and the transmission of messages), there is an exhaustive regulation in § 135 para. 3 StPO (Code of Criminal Procedure) and due to its severe interference with privacy rights a court order is necessary. On the one hand, this means that the content of messages cannot be determined by surveillance in accordance with other more general regulations (e.g. §§ 134 Z 4 StPO, 136 StPO ["optical and acoustic surveillance of persons"]). On the other hand, based on § 135 para. 3 StPO, neither locally stored data can be read out, nor can the Internet usage of the person concerned be determined, nor can data stored on a cloud be read out (see Heißl, Überwachungen und Ermittlungen im Internet, 147-149) as this information can be retrieved by securing the mobile device. Even messages stored on a provider's server whose transmission has already been completed (e-mail, WhatsApp) cannot be accessed by monitoring in accordance with § 135 para. 3 StPO. They are the object of securing (see Zerbes, Spähen, Spitzeln, Spionieren, 24-27, arguing that these data should not be secured at the provider but at the user. A certain confirmation of this view could also be seen in the Supreme Court's decision OGH 14 Os 51/18h).

Moreover, if the concerned person – also suspect – contradicts the securing of the device or data with regard to the right to remain silent this right cannot be circumvented. The evidence need to be stored at the court (or upon request at the prosecutor´s office) in a way that the information cannot

be read or amended until there is a decision about the use of the information /data as evidence (§ 112 Para.1 StPO).

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

§ 136 StPO would, in principle, allow the monitoring of the non-public behavior of persons. However, its scope of application is in any case limited by the leges speciales §§ 116 (banking transactions) and 135 StPO (surveillance of messages, see Introduction and Question 5) (Heißl, Überwachungen und Ermittlungen im Internet, 149). Furthermore, data stored on a device is not "behavior" that can be surveilled. However, calling up websites, using search engines, etc. does fall under this term and could therefore also be surveilled, based on § 136 StPO. "Technical means for image and sound transmission" or "image and sound recording" could be, in addition to cameras directed at the screen, also programs or material objects attached to the device (Heißl, Überwachungen und Ermittlungen im Internet, 149f.). In § 136 StPO, in addition to the possibility of a kidnapping (para. 1 Z1), above all the "major eavesdropping" in the context of organised crime or terrorist offences (para. 1 Z 3) is relevant (see Heißl Überwachungen und Ermittlungen im Internet, 150f.). A more extensive possibility of installing programs for the surveillance of (encrypted) messages was introduced with BGBl I 2018/27, but was repealed by the Constitutional Court with the decision of 11.12.2019 (G 72-74/2019-48, G 181-182/2019-18) that based its decision on Art. 8 ECHR.

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

If the cell phone is secured, the data (which can be the overall objective for securing the device, see OGH 14 Os 51/18h) can be read. If copies can be made, this has to be done and the device (as a mitigating measure) has to be handed over to the person concerned (§§ 110 Abs 4, 115 Abs 3 StPO; see also OLG Linz 20.7.2010 9Bs73/10i). According to prevailing opinion, copying the data itself by the authority is not considered as an additional act to secure evidence (see Schöch, Die Sicherstellung elektronischer Daten im Ermittlungsverfahren, Diplomarbeit,

https://epub.jku.at/obvulihs/content/titleinfo/4515658/full.pdf, 18). This is not applicable for messages and the surveillance of messages as there are specific regulations (see Question 5).

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

Any person who has objects to be secured must hand it to the law enforcement authority or to make the act possible in any other way (§110 StPO). This duty may if necessary, also be ensured by means of a search of persons or premises; in doing so §§119 to 122 StPO (general regulations concerning the search of persons and premises) shall apply. If information stored on data carriers is to be secured, access shall be granted to this information and, upon request, an electronic data carrier shall be provided in a generally used file format. Furthermore, the person must tolerate the production of a backup copy of the information stored on the data carriers (§§ 111 Para 1 and 2 StPO). By these regulations, the right to remain silent and not to incriminate oneself should not be circumvented (see Question 5)

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

If the owner is the suspect, he or she cannot be forced considering the right to remain silent and not to incriminate him-/ herself. For other persons it also depends if any procedural right applies (e.g. specific family members).

Other than that, the general regulations are in force, e.g. access to information should be granted. The law, however, only regulates the obligation to hand over the device and to provide the authorities with the relevant information, not to unlock a mobile device. If there is no cooperation with the authorities the law enforcement authority is authorised to use appropriate and proportionate coercive measures, to impose a financial penalty or present a court order for seizure to ensure the legal obligation (§§ 111 Para 1 and 2, 93 Para 2, 134ff StPO, see Question 8).

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

In any case, the owner/person in possession of the mobile device must be informed immediately or within 24 hours that the device was secured (§110 Para.4 StPO).

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

For evidentiary reasons devices/ data can be secured. The order comes from the public prosecutor's office and is executed by the law enforcement authority (§ 110 para. 2). The law enforcement authorities can act on their own initiative if it was found at the crime scene (§ 110 Para.3 cif. 1 lit. c StPO) or at the person or house search (§ 110 Para. 3 StPO). According to prevailing opinion, the law enforcement authorities can secure the evidence on their own initiative in case of imminent danger.

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

It makes a difference insofar as specific procedural regulations and rights apply depending on the status of the person concerned (see e.g., Question 5 and 9).

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.*

According to case law, it follows from § 111 para. 2 StPO (obligation to guarantee access to information stored on data carriers, if necessary by producing and delivering a data carrier) that the securing or seizure should also be able to guarantee access to the intangible object of information, even if the actual object of the seizure/confiscation is the data carrier as an "object" as defined in § 109 Z 1 lit a StPO (OGH 14 Os 51/18h). It follows that the original data carrier does not have to be the object of the seizure/confiscation (see also § 110 (4) StPO). Thus, a cell phone can be secured or seized on which copies of the relevant information are available or can even be produced.

The Supreme Court also expresses this in its ruling that data on cloud servers should be subject to Securing/seizure (OGH 14 Os 51/18h). As a result, this means that not only the locally stored data can be obtained through the backup/ seizure of a cell phone, but also any information that can be accessed by the cell phone. Thus, decisive "subject matter" is the data embodied on a file carrier

and not the file carrier that originally carries any data; this even applies to data stored on a cloud (§ 109 Z 1 lit a StPO; OGH 14 Os 51/18h).

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

If mobile devices or data is used for evidence the general evidentiary rules apply. Reference to hostage taking, organised crime and terrorism applies for the use of messages and other information as evidence (esp. seizure; §§134 ff StPO) that can be only obtained by measures that severely interfere with rights (esp. Art. 8 ECHR), but not for other securing activities. In order to retrieve evidence from messages, the mobile device needs to be seized. Accordingly, more information will be provided below under Questions 16-36.

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.*

See below Section 3

Mobile device seized

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

In principle, the same rules apply to the seizure of cell phones as to any other seizure. Here the reason of § 115 Abs 1 Z 1 StPO is of particular interest, namely that the cell phone is required as evidence in further proceedings. This is a special standardization of the proportionality requirement of § 5 StPO. In accordance with the principle of proportionality, seizure is only admissible if no copies can be made or would not fulfil the purpose of evidence (see §§ 110 para. 4, 115 para. 3 StPO; see also OLG Linz 20.7.2010 9Bs73/10i).

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

See Question 11 and the seizure is seen as the maintenance of the securing by order of the court (§ 109 Z 2 StPO). There are specific regulations when it comes to the surveillance of messages. In such cases, the seizure is necessary. More concretely this means:

Data concerning the transmission of messages (§ 135 (2) StPO):

In this context "messages" means information sent over a communications network or an information service society.

If the owner of the device explicitly consent to the use of data the information concerning the transmission of messages can be retrieved if concerns an intentional act that is possible punished with more than six months of imprisonment (Z2). Without the consent of the owner the information about data concerning the transmission of messages is possible

- if and for as long as there is a strong suspicion that a person affected by the information has kidnapped or otherwise taken possession of another person, and the information is limited to the data of such a message which can be assumed to have been transmitted, received or sent by the suspect at the time of the deprivation of liberty (Z 1)
- if it is an intentional offence with a possible penalty of more than one year of imprisonment and there is a well-founded expectation that data of the suspect can be determined (Z 3) or
- If the basis is an intentional act with a possible penalty of more than one year of and the collection of data is necessary to determine the whereabouts for fugitive suspects (Z4)

Surveillance of message content itself (§ 135 para 3)

In this context "messages" means information sent over a communications network or an information service society.

If the owner expressly agrees the same applies as under para 2 (Intentional act and more than 6 months of possible imprisonment (§ 135 para 3 Z 2 StPO). Without the consent of the owner the surveillance of messages is possible:

- In case of hostage-taking (Z1; see above)
- If it is an intentional offence with a possible penalty of more than one year of imprisonment and the surveillance is required to solve the offence or the investigation or prevention of crimes committed by criminal or terrorist groups would otherwise be considerably more difficult and
    - the the owner of the technical equipment that was or will be used to transfer messages is urgently suspected of having committed on of the mentioned offences or (Z3 lit a)
    - it is to be expected that suspected person will use or connect to the technical equipment (Z3 lit b)
- If the basis is an intentional act with a possible penalty of more than one year of and the collection of data is necessary to determine the whereabouts for fugitive suspects (Z4; see above)

Moreover, the law in §§ 137 para 3 and § 138 para 1 StPO specify that the measures can only be upheld for a period that is necessary to achieve the objective. Moreover, there are strict requirements how specific the measures has to be described (e.g., name of the owner, the place of the surveillance, technical means to be used, period of time).

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

If the concerned person – also suspect – contradicts the securing of the device or data with regard to the right to remain silent this right cannot be circumvented.

As the seizure is the judicial decision on the grounds or continuation of securing evidence thus the rules for securing information apply accordingly (§§ 109 Z 2; 114 para. 3 and § 110 para 4 StPO; see above Question 5 and 7)

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?*

Additional substantive criteria may arise from the fact that the seizure would circumvent other rules of gathering evidence. This is particularly relevant with regard to the right to remain silent (§157 (2) StPO; cf. also the possibility of an objection under Section 112 StPO), but, particularly important in this context, also for the surveillance of communications/messages. Here the provisions of § 135 must be complied with (cf. Bauer, Verwertungsverbote zur Gewährleistung von Waffengleichheit, 162f.), although this does not apply if the messages are stored on the device or on an external server and the owner(s) of the device already had access to them (then it is no longer a matter of surveillance of messages, cf. Zerbes, Spitz, Spähen, Spionieren, 25).

Important are also data protection considerations, secrecy of telecommunication and protection of the home. In this context, the problem area cell phones and the protection of the home can be elaborated as follows: There are three possibilities, how the access to a cell phone could intervene in the right to protection of the home (interpreting 8 ECHR and the national regulation broadly):

1) A house search could be ordered, in order to secure or evaluate a cell phone (see § 119 para 1 StPO)

2) If a house is to be entered in order to attach hardware to a cell phone that allows the monitoring of the behaviour of the person concerned (cf. for this purpose § 136 StPO and the section on online searches), this is an infringement on the protection of the home. So far, the ECHR has abstained from the question of whether there is an infringement to the protection of the home in addition to the infringement with private life that already exists. The national law (HausrechtsG) does not seem to be applicable due to the lack of house search (see Heißl, Grundrechtskollisionen, 366-371).

3) A surveillance of the house could be carried out by using the hardware of a terminal device (e.g., a cell phone) (based on § 136 StPO).

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

The owner's consent to access the cell phone is only required if the requirements of § 115 para 1 are not met (data or device necessary in the further proceeding as evidence). Provided that all

persons having a right to the object agree to the access by the authorities, they do not have to rely on the permission to interfere with § 115 StPO, since no right is interfered with.

Specific regulations concern messages /communication. The obligation to comply with the requirements of Section 135 of the Austrian Code of Criminal Procedure (StPO) is likely to be particularly relevant with regard to messages that the person concerned receives after losing access to his or her cell phone. In the case of § 135 para. 3 no. 2 in conjunction with para. 2 no. 2 StPO, the consent of the owner of the cell phone may then be required (otherwise the regulations of the securing and seizure hast to be applied and assessed again).

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

See above Question 9.

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

For the seizure of the device and data see Question 10. Concerning the surveillance of messages, the following applies: The prosecutor has to inform the suspect or any other person who was concerned about the measures and the court order. This can be delayed if the investigations (or other cases) so require (§§ 138 para 5 StPO).

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

The tracing of data about message transmissions (and also about the mere willingness to do so, see OLG Vienna 3.2.2017, 20 Bs 4/17k; OGH 5.3.2015, 12 Os 93/14j (12 Os 94/14m) is possible by requesting information according to §§ 134 Z 2, 135 Abs 2 StPO.

On the use of the frequency cell report the Supreme Court set the limits (5.3.2015, 12 Os 93/14j; 12 Os 94/14m), the use of an IMSI-Catcher is regulated under 134 Z 2a, 135 Abs 2a StPO (before that the topic was alreads dealt with by the Regional court Vienna 3.2.2017, 20 Bs 4/17k).

The storage of data (against deleting it) is regulated under §§ 134 Z 2b, 135 Abs 2b StPO.

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

See Questions 12 and 17.

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.*

See Question 13.

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 Question 13.

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?*

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?*

Service providers have to support the investigative authorities in case of information about data concerning messages as well as surveillance of messages that is performed upon a Court order (§ 138 para 2 StPO).

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

See Question 17

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

See below Section 3

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: Worth mentioning are cases where objects, i.e. mobile devices are found "accidentally", meaning that it was not intended to secure them e.g., during person or house searches. In these cases, the police can secure them if they might be linked to a criminal offence and the police includes it in the protocol and inform afterwards the public prosecutor immediately (§122 StPO). The prosecutor has to decide if a seizure and a court order are necessary or if the mobile device is irrelevant for the case. In any case, the person concerned has to be informed about the search and the outcome (122 para. 3 StPO; Berger, Verwertungsverbote, p. 128).

Overall, it is important to differentiate between securing the mobile device to collect data from it and the seizure (court order) if the securing should be maintained in order to secure evidence (e.g. SMS, messages, E-mails stored on the phone, etc.) on the one hand. On the other, there are information about data concerning the contract and IP addresses (§ 76 a StPO, least severe interference) and information about data concerning messages (traffic, access and location data) as

well as the surveillance of messages (§ 135 para 2 and 3 StPO, most severe interferences; see Question 5). The latter are connected to much stricter requirements and reporting obligations.

***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: According to § 127 Para. 2 StPO and the regulations for "Behaviour when reporting findings and expert opinions, in particular on behalf of a court (public prosecutor's office, administrative authorities)", all findings have to be documented appropriately and in a way that corresponds to the acknowledged rules and methods used in that specific area of expertise.

***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: There is no explicit regulation in the national law.

***33.* Question:** *What are the main legal issues in your jurisdiction in the cases when mobile devices are involved in crimes across geographical boundaries? What procedures are foreseen to tackle these multijurisdictional issues? Should the forensic examiner be aware of the nature of the crime and the regional laws/legislative framework?*

Answer: The general rules on cross-border cooperation also apply for cases when mobile devices are involved.

***34.* Question:** *Is there an established procedure/course of action to decide whether to apply the EIO or another instrument for cross-border gathering of evidence within the EU?*

Answer: This decision depends on the same rules and consideration as every investigative measure. The decision is taken in every case individually based on the needs of the investigation.

***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: If the case so requires the application of MLAT is possible under the general rules.

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

Answer: Cooperation with the private sector is common, but mainly when it comes to receiving information about the contract partner (and in specific cases to cooperate when it comes to the surveillance of messages or information on data concerning messages).

§ 76 a StPO regulates the information about master and access data. Master data is such personal information that is necessary for establishment, processing, modification or termination of the contract between the user and the operator of a communications service, such as name, address, competitor number or creditworthiness of the user. However, only such data is recorded, which can be obtained without the evaluation of data traffic. In this context the legal requirements are less strict than concerning internet communication (§ 76 a para 2 StPO) or the access to information about data concerning messages (§ 135 para 2 StPO).

§ 76 a para 2 StPO lists the information that is accessible for the prosecution organs, thus such data that is necessary to identify a participant in the internet communication. This includes personal information about the owner of a particular connection, i.e. the information which subscriber is connected under an already known IP address (Bauer, Verwertungsverbote, p. 202).

Until July 1, 2014, providers of public communications services had collected extensive data in connection with telecommunications from their production or processing until six months after completion of the communication act. These provisions on data retention were amended with the decision of the Constitutional Court of 27. 6. 2014,G 47/12 ua, as unconstitutional, whereby this repeal became effective as of 1. 7. 2014. Since then, the data concerned may no longer be used by the law enforcement authorities.

Information about data concerning messages (§ 135 para 2 StPO) may be requested to the operator of the telecommunication service or the respective private communication participant. In the second case, the access can be granted for example by securing a cell phone or computer on which the relevant information such as call lists or e-mail addresses are saved. Since the operator of the telecommunications service is not involved in this type of access, this is a security measure in accordance with §§ 109 ff StPO, for which the requirements of §§ 134 ff stop do not need to be met (Berger, Verwertungsverbot, pp. 202f; see question 5).

Contact is rare when it comes to the seizure or confiscation of the device and related measures that are taken to retrieve date from the device. In these cases, expert witnesses are assigned.

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: Any interference with the acquiring of information related to communications constitutes an intervention in Art 8 ECHR, regardless of what happens to the retrieved information afterwards (see ECtHR 30.7.1998, Valenzuela Contreras, 27.671/95,). Interference in this context can be: Identification, storage and transmission of personal data as well as access thereto. Each of these processes represents a separate interference (see EGMR 29.6.2006, Weber & Saravia, 54.934/00 = NLMR 2006, 177, Rz 79, Heißl, Grundrechtskollisionen, 301f.) that can be justified in specific settings.

The processing and analysis of personal data by law enforcement authorities, prosecutors and the court need to be lawful and proportionate (§§ 74 together with 5 StPO). Further, the use of data is subjected to general data protection regulations. Data that is obtained unlawfully needs to be deleted immediately as well as when the interest of the person concerned outweigh the public interests in further storage. Overall, data can only be stored for 60 years at maximum (§ 75 para.3 StPO; VfGH 29.06.2012, G 7/12; see also § 27 DSG 2000).

The acquisition of data by mere calling up of public homepages, chat forums etc. is not yet an infringement with fundamental rights. However, it will be if the data obtained is stored or systematically evaluated. The same applies to the use of search engines (see Heißl, Grundrechtskollisionen, 313).

In the context of information about data concerning messages and the surveillance of messages, the suspect can request to delete all stored and retrieved information if they can/ are not used in the proceedings. This right also corresponds to other persons if they are concerned, e.g., can be seen or heard (§139 para 4 StPO). See on information about /surveillance of messages also Questions 5 and 19.

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: see above

***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: There are the strict general regulations how evidence can be obtained. Moreover, as other jurisdictions also the Austrian law differentiate between prohibitions on the collection and use of evidence. The prohibition of the collection of evidence mainly relates in the context of mobile devices to the use of information that are protected by the right to remain silent and not to incriminate oneself or a close relative (§156 StPO) as well as to the prohibition to circumvent these rights (see also above Questions 5, 8-9 and 18-19). This is not excluding observations of the suspect or their relatives. Relatives can even be optically and/or acoustically surveilled, if it can be assumed that there is contact between the concerned person and the suspect and the clarification of the suspected crime otherwise has no chance of success or at least would be considerably more difficult. In this respect, information may come to light which was provided directly by the relative and in accordance with § 156 para. 1 Z 1 could not have been obtained (Bauer, Verwertungsverbote, p.4).

According to § 140 para 1 StPO, evidence collected through the request for information about data concerning messages (§ 135 para 2 StPO) and the surveillance of messages (§ 135 para 3 StPO) can only be used as evidence if the measures have been lawfully ordered and authorized (§ 140 para 1 Z 2 StPO). Accordingly, it is necessary to have a judicial authorization, an order of the public prosecutor's office and the authorization of the legal protection commissioner. In addition, the material requirements of § 135 StPO must have been met without whose existence the monitoring could not have been lawfully ordered.

In additon for the cases of § 135 para. 2 and 3 StPO (excluding in both cases hostage taking; see Question 17) if it serves to prove an intentional punishable act for which investigative measures were order or could have been ordered (§ 140 para. 1 Z 4 StPO).

For further information on evidence see Question 40.

***40.* Question:** *What if procedural rules are not followed? Can evidence from mobile forensics still be submitted to the Court in certain circumstances, balancing out the interest of the criminal justice with the severity of the procedural breach?*

Answer: If evidence is obtained despite the prohibition of the collection of evidence, it can also not be used in the following procedure, e.g., if the information comes from a confidential talk that is protected under law (Bauer, Verwertungsverbote, p.7) as otherwise this could provide a ground for annulment (see § 281 StPO).

When it comes to the violation of procedural rules, the law differentiates between cases that can serve a ground leading to an annulment and violations of procedural rules that are considered less severe (e.g., access to case files) and need to be objected or appealed in order not to be used in the further proceedings (see e.g. § 281 and 106 StPO). According to the ECtHR, the overall procedure has to be fair (see Section 5).

In these constellations, also the equality of arms plays an important consideration (Bauer, Verwertungsverbot, pp. 63ff). Accordingly, as a rule, evidence that is collected unlawfully cannot be used in the further hearings (e.g. unlawful house search). In these cases, the evidence cannot be used, also because the criminal law does not have a principle for truth exploration at any price that would allow evidence to be submitted that was collected by violating rules concerning evidence. (Bauer, Verwertungsverbot, p. 64). If specific procedural rules – that are not considered to be grounds for annulment - are not followed this has to be objected or appealed in order for the evidence not be used or put into perspective (§106 StPO; e.g., specific procedural rights during investigations and questioning like access to case files).

***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: see Questions 13 and 25ff.

***42.* Question:** *What are the consequences if mobile evidence are altered either intentionally, or unintentionally due to their dynamic nature during the investigation process? Note that intentional alteration refers to using a process to uncover data which is known to alter some (meta)data, not to the falsification of evidence. The question is more whether any alteration, even on small and not relevant data may render the evidence inadmissible.*

Answer: The use of mobile devices and the corresponding data as evidence follows the general rules. Accordingly, new evidence can be brought forward reflecting the general regulations governing evidence. The seizure and securing – and the corresponding permissions – are valid for the device and corresponding data as they are at the point that the act is set. If new evidence is produced afterwards, this has to be secured and seized according the law (See also Question 20).

***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: Experts has to produce their statements and expert opinions according to their best knowledge and the state of the art in their respective area of interest. If the statement or expert opinion does not correspond to these requirements or there is a contradicting opinion the experts has to be questioned. If the questioning do not lead to a satisfactory outcome another expert should be involved (§ 127 para.3 StPO; see specific regulations for expert witness

es in the area of IT: https://www.gerichts-sv.at/ps.html, 68).

***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 other specific case law as stated under the Questions is known in this context.

***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: The regulations for evidence is applicable to all forms and type of evidence. The general regulations can be found in the CCP as well as more specifically on the regulations concerning expert opinions. The latter include a reference to the state-of-the-art methods and tools of the respective area of expertise (see Question 43).

***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: It depends on which regulations an interference takes place and if those are absolute in nature. Otherwise the interference might be lawful and necessary (e.g. Art. 8 ECHR). See Section 2.

***47.* Question:** *Is there case law in your jurisdiction on evidence collected through mobile forensics having been questioned or rejected in Court because the admissibility was questioned? If yes, please elaborate on at least 3 cases.*

Answer: No other specific case law as stated under the questions is known in this context.

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

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

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

Answer: Mobile forensic evidence´s value is decided according to the general rules. The judge can decide based on the principle of free appreciation how much value is given to specific evidence. Thus, on the question whether a fact is to be accepted as proven, the judges do are not bound by specific regulations (e.g., at least 3 witnesses, etc.), but decide only according to their free conviction gained from the conscientious examination of all evidence submitted for and against. The court must carefully and conscientiously examine the evidence for its credibility and probative value both individually and in its internal context (§ 258 para 2 StPO). However, in practice expert opinions have considerable weight for the judgement (Berger, Verwertungsverbote, p. 184 with further references).

Experts are to be appointed if investigations or the taking of evidence require special expertise which is not available to the law enforcement authorities (§ 127 para 1 StPO). Thus, it is not a prerequisite, but especially when it comes to more complex procedures to secure evidence from mobile devices expert witness can be involved. There is a list of certified expert witness for relevant areas of expertise and primarily those should be appointed (§ 127 para 2 StPO).

The concrete task concern: The forensic data backup or also computer forensics or digital forensics deals with the strictly methodical investigation of suspicious incidents in connection with IT systems on data carriers and in computer networks for the clarification. It includes the determination of the facts and the suspects by acquisition, analysis and evaluation of digital traces in computer systems (e.g., forensic investigations and procedures also for the processing of support cases, i.e. hardware and software failure and incorrect operation by the User). Moreover, evidence, for example, data carriers, are secured as well as protocols of the network traffic are secured and analyzed. Besides the classical disk analysis of hard disks from PC and server systems also includes evaluation of digital traces in smartphones and PDAs.

Moreover, the work also deals with data recovery and reconstruction. This means the recovery of original data after a data loss on a media in the narrower sense as well as the detection of incorrectly transferred data units and their recovery in a broader sense. Through external influences (mechanical damage, strong electromagnetic fields, sunlight at optical data medium, natural disasters, etc.), data on storage media can be changed or become unusable. However, the cause can also lie in the misbehaviour of data users by accidentally or intentionally changing data can be done, for example, to cover up traces.

Data evaluation or data analysis summarizes such techniques, which recognition of patterns or the search for structures, microstructures and enable special features exploratively. Data analysis is primarily about assessing, preparing, and presenting existing data and to extract einformation thereof (https://www.gerichts-sv.at/ps.html, 68).

In order to be certified, as a minimum requirement the person needs to have at least ten years, preferably professional activity in a responsible position in the or a related area of expertise immediately before registration; a five years of activity of this kind is sufficient if the applicant holds a university degree or has completed corresponding studies (with some exemptions existing; see: https://www.gerichts-sv.at/ps.html, 68).

The exam concerns following areas e.g: incident analysis, post-mortem analysis, live forensics, key elements for forensic processes, forensic duplication, CERT taxonomy, basic structure of disks and file systems, structures for storage organization, filecarving, concepts of data protection, RAID systems, Bare-metal restore, cloud computing storage, knowledge of the current software packages for acquisition and evaluation like Encase, FTK, CTK etc. (see: https://www.gerichts-sv.at/ps.html, 68).

***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 other specific case law as stated under the Questions is known in this context.

***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: See Question 48

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

Answer: No other specific case law as stated under the Questions is known in this context.

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: In order to safeguard the respect of the principle of equality of arms the law foresees the right to submit applications for evidence to defend oneself (§ 55 StPO, see also Question 59). Furthermore, if evidence is obtained in a way that is not in line with the law, in order to ensure the respect of equality of arms this evidence cannot be used in the procedure under specific circumstances (see Question 40). According to the ECtHR in order to ensure a fair trial and to respect the principle of equality of arms the overall proceeding has to be fair (Bauer, Verwertungsverbot, pp. 24-31). Accordingly, there are some severe violations of the rules to obtain evidence that cannot be used in the further proceedings without producing the basis for an annulment. Others can be "healed" during the proceedings if the overall proceeding is considered fair (Bauer, Verwertungsverbot, pp. 32ff).

Also, the position of expert witness is worth mentioning. They are obliged to be independent, however, they are ordered either by the prosecutor or the court (from the list), thus, creating an indirect dependency. Moreover, suspects and accused cannot order but just a private expert witness who however is only considered as a "regular" witness, but not as an expert witness (Berger, Verwertungsverbote, p.185).

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: This question cannot be answered in the framework of this research.

***53.* 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: The expert shall comply with the time limits given to him by the court (by the public prosecutor's office or the administrative authority) for his expert work. In particular, the Expert shall immediately after his appointment check whether he can reliably fulfil the assignment given to him within the time limit set ("Behaviour when reporting findings and expert opinions, in particular on behalf of a court (public prosecutor's office, administrative authorities").

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

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

5.1 The Prosecution

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

Answer: The same as for all other sort of evidence.

5.2 The Court

***56.* 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: see Section 3

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

Answer: see Section 3

5.3 The defendant and defender

***58.* 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: The right to access the case files is one of the basic rights in the StPO (§ 49 StPO) and should be ensured from the beginning of the investigations (§ 53 para. 1 StPO). The right to access the case files also includes the right to make copies of the evidence if their possession is not illegal (§ 52 para 1 StPO). According to the StPO, access to case files can only be denied in special cases, namely to avoid serious danger to the life or rights of another person (§§ 51 Abs 2 iVm 162 StPO), a threat to ongoing investigations (§ 51 para. 2 StPO), to the protection of an important interest, as well as to avoid the impairment of national security (§ 77 StPO). By the decision of the Supreme Court, it is now established that a blanket reference to the endangerment of the current investigation procedure is not sufficient to to refuse to grant access to the files. Rather, a clear description of certain circumstances is necessary for the fear of such a danger (1.1.2013, OGH, 14Os43/13z). The restriction of the access to the case files can be maintained as long as the purpose of the investigation procedure requires, but at the latest until the end of the investigations (§ 51 para. 2 StPO).

In addition, certain investigation files can be categorized as classified information (Verschlusssachenverordnung, BGBl. II Nr 3/2015). This provision applies primarily to investigation files in which there is a particular interest in secrecy, in particular information about data about messages communication (§ 135 Abs 2 StPO), surveillance of messages (§ 135 Abs 3 StPO), acoustic monitoring of persons, i.e. so-called "eavesdropping attacks" (§ 136 Abs 1 Z 2 and 3 StPO) and goes with the restrictions in § 51 Abs 2 StPO (§§ 1, 2 Classified Information Ordinance).

If the right to inspect files is unlawfully denied or restricted a complaint has been lodged, the appeal of an objection of infringement of rights may be lodged with the court before the end of the preliminary proceedings (§ 106 Z 1 StPO). Appeals against court decisions and authorizations may be lodged in accordance § 87 StPO can be filed.

(Zach/Katona/Birk: Die ersten 48 Stunden (2018) pp.64ff)

When it comes to the information about data concerning messages (§ 135 para 2 StPO) or the surveillance of the messages (§ 135 para 3 StPO), the suspect has the right to see and listen to the results (§ 139 para 1 StPO). Here again the suspect has the right to request the use of additional materials for his/her defence if the evidence can be used before the court (§139 para 3 StPO, see also Question 52)

5.4 Witnesses

***59.* 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: Under specific circumstances witness do not have to testify (i.e., if they would incriminate themselves or a relative) and no measures should be taken if they would circumvent these rights (see e.g., Question 39). Moreover, witness have the right to be informed if their mobile device is secured or seized (see Questions 10 and 22). In addition, if a person is concerned by the information of data concerning messages or the surveillance of messages, she/he has the right to access the files (§139 para 2 StPO). In this context they also have the right that information is deleted if they are not relevant for the proceedings or were obtained unlawfully (§ 139 para 4 StPO; see also Question 58).

5.5 The Victim

60. **Question:** *How are the victim's/victims' rights ensured during both the pre-trial and the trial phase of the proceedings? How is their privacy preserved? Can they use the evidence obtained via mobile forensics when exercising their rights? Please refer to case law if possible.*

Answer: Here the general rules on victim´s protection and rights apply. If sensitive date is part of the investigation and part of the files, this information can be excluded and classified. Copies must be made in which the identity and other relevant circumstances have been made illegible (§ 51 para 2 StPO).

Also, victims have to be identified if their mobile devices were secured or seized; or if they were concerned by the information about data concerning messages or the surveillance of messages (see Question 59).

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: N/A

Version 1: 16.11.2020