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

IMPORTANT TO READ BEFORE ANSWERING THE QUESTIONNAIRE:

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

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

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

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

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

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

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

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

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

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

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

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

Introductory questions:

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

Answer: Indication of length of answer: one line.

István Ambrus PhD, associate professor in criminal law, Eötvös Loránd University, Faculty of Law, Department of Criminal Law

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

Answer: Indication of length of answer: one line.

Egyetem square 1-3,1053 Budapest, Hungary

3. **Question:** *Do you have a legally defined term for a "mobile device"? If yes, what kind of devices are included within it? (e.g. Smartphones, Tablets, Smartwatches, Cameras, MP3-players, Navigation devices, Drones)*

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

In Hungary we do not have a general legal definition for mobile devices. Instead we can find the mentioned tools in several various acts.

First of all, from the point of view of substantive criminal law – accordingly to the regulation of Directive 2013/40/EU – Article 459 paragraph 1 point 15 of the recent Hungarian Criminal Code (Act C of 2012, in force since the 1st of July 2013, hereinafter: HCC) defines "information system" as a device which ensures the automatic processing, management and storage of electronical data. Thus in the field of substantive criminal law, if we are dealing with for instance a smartphone, a camera, a drone, etc. we can usually consider these devices first of all as individual information systems. Of course these devices also can be considered as "things" in the case of criminal offences against property. From this point of view, a mobile device as a physical tool can be the object of for example theft, embezzlement, etc.

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

In the field of criminal procedural law, a mobile device can be considered as an 'physical evidence' [Code of Criminal Prodecure of Hungary, Act XC of 2017, in force since the 1st of July 2018, hereinafter: HPC, Article 165 point 'e'], if we are talking about the device itself (eg. a cell phone), or 'electronical data' (HPC, Article 165 point 'f'), if the object of the observation is not material but a kind of software (like a mobile application).

We should mention the 12/2018. (VI. 12.) Ordinance of the Department of Justice on the regulation of some of the criminal procedural actions and persons participating in criminal proceedings. This Ordinance mentions 'mobile device' in an explicit way twice. First time in Article 22 paragraph 1, which states that during the examination of the documents of the criminal proceeding the authorized person has the right to make a copy of the documents with his/her camera, handheld scanner or mobile device. Secondly in Article 45 paragraph 6, which states that suspect and the defence lawyer have the right to talk to each oder via a cell phone or other mobile device if they are not on the same place during some part of criminal proceeding. Thus it could be not just a mobile phone but for instance using Messenger, Skype, etc. with a tablet. Although the general definition of mobile device is still not regulated nor in this Ordinance.

Finally the 57/2013. (XII. 21.) Ordinance of the National Police Headquarters defines "mobile device" (but only in the application of this ordinance) as a device which is capable of running and performing the functions of the "Robot Zsaru" NOVA Activity Management System Mobile Framework in order to support public policing (the definition is in force since the 26th of May 2017). Although this is a very special definition used by only the police, so it irrelevant in this questionnaire.

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?*

As I already mentioned previously, the source of these rules basically is the HPC. According to the regulation of this code, a mobile device can be considered as physical evidence or electronical data, although if the question is about the materials downloaded or sent by the device (for instance a Messenger conversation), it seems much proper to deal with the regulation of electronical data.

The investigation authority has a right to search for evidence in a home or other premises or vehicles. During the search it is also possible to examine the materials on information systems (like a computer, a tablet or a cell phone, see HPC Article 302 paragraph 1).

Search may be ordered if there are reasonable grounds for believing that it leads

a) to apprehend the perpetrator of a criminal offence,

b) to detect traces of a criminal offence,

c) to find a means of proof,

d) to find something to be confiscated; or

e) to examine the information system or data carrier (see HPC Article 302 paragraph 2).

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

It also possible to fulfil a "body search" if there are reasonable grounds for believing that the involved person holds some kind of evidence in his/her clothes or body (HPC Article 306 paragraph 1). Thus it could be possible to find the cell phone in somebody's pocket, etc.

If the search or the body search is successful the materials on the mobile device can be read by the authorithies.

It has to be noted that as a general rule, in order to conclude an identity check or a body search, the reason has to be specified [eg. to defend the public interest; see Act XXXIV of 1994 on the Police, section 29., subsections (1) and (6)]. However, the Police Commissioner may order a 'special monitoring' regarding numerous counties or the whole country, where an identity check and a body search does not necessarily require a specified reason [Section 26 subsection 1, and subsection 2 paragraph a)]. The Police Commissioner usually orders these special monitorings regarding numerous counties for several months. Between 2015 and 2017, the entire country was under "special monitoring", which was criticized by numerous Hungarian Civil Society Organizations (for further reference: a FAQ by the Hungarian Civil Liberties Union can be found here in Hungarian: https://tasz.hu/cikkek/fokozott-ellenorzes-fokozott-jogsertes; a detailed paper was published in 2008 by the Hungarian Helsinki Committee: https://helsinki.hu/wp-content/uploads/books/hu/Szigoruan-ellenorzott-iratok.pdf)

Furthermore, electronical data could be of course seized (HPC Article 308 paragraph 3). But it is not the case then the court, the prosecutor and the investigation authority (usually but not always the police) has the right the oblige the owner of the electronical data to preserve it ("obligation to preserve electronical data", HPC Article 316 paragraph 1). The obliged party has a duty to preserve the electronical data in the same condition as it used to be at the time obligation (HPC Article 316 paragraph 4).

Finally we have to mention the regulation of "hidden investigation" by the police. These rules can be found in Act 34 of 1994 on the Police. According to Article 74 point 'e' of this code, the police

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

has the right – with the permission of the court – to observe information systems in a hidden way, also to read and record the data found in these systems.

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?*

The limits of the search during criminal proceeding are the following.

The search of the office of a notary public or a law office – if it concerns professional secrets related to the work of notary or defence counsel – shall be ordered by the court. During this search the presence of a prosecutor is mandatory (HPC Article 303 paragraph 2).

If the objective of the body search is to find a designated object, the person to be searched shall first be demanded to surrender the subject of the search, and if such demand is obeyed, the body search shall be omitted.

The body search cannot be fulfilled in an obscene way.

Ventricles can be only searched by a doctor.

And finally, except of urgent cases the body search can be only fulfilled by a person with the same gender with the searched person (HPC Article 307).

So according to the mentioned rules, the limits of the search is based on private life and sexual freedom, but not on the nature of the committed criminal offence.

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

It is not precisely described in HPC. Although according to the Preamble of HPC, the goal of this code is to state the responsibility of criminal offenders and also to find out the truth. Furthermore

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

the aim of search, body search and seizure is to find and ensure evidence about the commitment of the criminal offence. Thus the investigation authority is allowed to do so, because this possibility can be led down from the other, more general rules and principles. Also if it would not be allowed, this situation could make impossible for the authorities to fulfil their duties prescribed by the law.

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

If the found information carries the sign of criminal activity and therefore the seizure seems necessary, the investigation authority has the right not just to read but also to make a copy of the found data (HPC Article 308 paragraph 3).

We can also cite the regulation of *minutes* according to this question. HPC Article 358 paragraph 2 allows for the prosecutor and the investigation authority to order the recording of the investigatory action by a video or audio recorder or other equipment.

Finally the 11/2003. (V. 8.) joint Ordinance of the Department of Justice, the Department of the Interior and Treasury Department states in Article 67 that seizure of electronical data could be fulfil by copying (in force since the 1st of July 2018).

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

No, it is not. HPC Article 305 paragraph 5 states that anyone interfering with the measure taken in order to perform search, body search or seizure may be forced to tolerate such measures and – with the exception of the defendant – may be subject to a disciplinary penalty.

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

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

It is not regulated in an explicit way, but according to the aim of criminal proceedings and these legal institutions, he/she can be forced to do so (not bodily but legal force; see question 6). If he/she will not, a disciplinary penalty could be imposed. If it is not possible to unlock the device by the owner/person is possession (he/she do not cooperate despite the imposition of the disciplinary penalty; he/she forgets the password or he/she disappears during criminal proceedings) an informatician expert should unlock an examine the mobile device (HPC Article 188 paragraph 1).

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

It is not regulated in an explicit way, but according to the aim of criminal proceedings and these legal institutions, it is not necessary (see question 6).

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

The court, the prosecutor and the investigation authority (commonly the police) all have the right to do so. To formal requirements see question 4. To some exceptions see question 5.

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

It is not important, but the accused person cannot punished with a disciplinary penalty if he/she tries to obstruct the search (see question 8).

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.*

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

There are not any special regulation for this issue, thus only the mentioned ways can be followed during a criminal proceeding related to data stored in a Cloud.

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

According to the answer on question 13, there are not any. Although we should mention that HPC Article 337 regulates a special opportunity in the case of terrorism (HCC Article 314) and child pornography (HCC Article 204). This is called "temporary prevention to access electronic data". It can be applied if the investigation is in progress because of the mentioned felonies and if for example the person who was obliged to remove the electronic data will not do so, etc.

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

The Hungarian evidentiary procedure is conducted to find the truth of the facts because the criminal responsibility of a person must be found upon the factual truth. Hungarian regulation of criminal proceedings is based on the principle of free evaluation of evidence, so the main rule is that using evidence to prove the truth is free. Although HPC catalogues the means of proof and the rules of exclusion of evidence.

The lawfulness of the evidentiary procedure is a substantial interest, the human dignity, the personal rights and the right of reverence of those involved shall be respected in the course of the acts of the evidentiary procedure, and unnecessary disclosure of private data shall be prohibited (HPC Article 2).

HPC Article 167 paragraph 1 states that in the course of criminal proceedings, all means of evidence specified by law and all evidentiary procedures may be used without restriction. HPC Article 167 paragraph 3 also states that the court and the prosecutor shall freely weigh each piece

of evidence separately and collectively and establish the conclusion of evidence based on their belief thus formed.

Although HPC Article 167 paragraph 5 states that facts derived from means of evidence obtained by the court, the prosecutor or the investigating authority by way of committing a criminal offence, by other illicit methods or by the substantial restriction of the procedural rights of the participants may not be admitted as evidence.

This provision covers two main types of exclusion: an absolute and a relative exclusion. The evidence is excluded by all means if it is obtained through a criminal offence. Also the absolute exclusion as a consequence can follow if the authorities are using other illegal methods during the criminal procedure.

The violation of procedural right of the participant can also lead to exclusion, but this exclusion is relative. It means that the exclusion can only occur if the restriction of the mentioned right was significant. It belongs to the competence of the court to judge whether the violation was substantial, and the court is not obliged to exclude the evidence only on the fact of an infringement.

Not following the mentioned rules during the examination of a mobile device (eg. a search of a law office which is leading to find a mobile device, but without the presence of a prosecutor) can be considered as a relative reason of exclusion, thus it is always up to the court in the concrete case to exclude the evidence got that way or not.

Mobile device seized

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

Yes, a mobile device can be considered as physical evidence or electronic data (see question 4). Both of them can be seized based on the regulation of HPC Article 308 paragraph 3.

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

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

The court, the prosecutor and the investigation authority all have the right to order seizure.

The seizure shall be ordered for those movable things, account money, electronical money or electronical data, which

a) are evidentiary means,

b) can be confiscated. (HPC Article 308 paragraph 2)

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

HPC Article 302 paragraph 2 point 'd' states that a search can be ordered if there are reasonable grounds for believing that it leads to find something to be confiscated. And confiscation as a criminal sanction (regulated in HCC Article 72-73) can be only imposed if the involved thing has been previously seized during criminal proceedings (HPC Article 308 paragraph 2 point 'b').

During proving process the seized mobile device should be available, thus it can be always searched. According to HPC Article 316 paragraph 6 it is also possible to copy information into an information system owned by the authorities. Also see question 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?*

There are not any special rules for this issue. HPC Article 316 paragraph 7 only states that the materials on the seized mobile device can be only read by the court, the prosecutor, the investigation authority (as a main rule). At the request of the owner of the device, a certified copy

shall be issued on the electronical data which can be found on the seized device, unless this jeopardises the interests of the procedure (HPC Article 315 paragraph 6).

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

No, the consent of the owner/person is possession is not an element of seizure.

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

It is not regulated in an explicit way, but according to the aim of criminal proceedings and the legal institution of seizure, he/she can be forced to do so (see question 6 and 9).

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

Seizure must be ordered in an official decision. In this decision the owner/person in possession should be informed about the time, scene and object of seizure and also about his/her right to file a complaint against the decision (HPC Article 369 paragraph 1).

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

There is not any explicit regulation for these issues but according to the aim of HPC it these tools should be allowed to use.

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

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

No, it is irrelevant.

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 are not any other options just the two mentioned.

Although the before-mentioned legal institution (see question 14) "temporary prevention to access electronic data" can be ordered by court in the case of some special, serious felonies (like terrorism, child pornography, drug trade, etc.). It is possible – beside other cases – if a request for legal assistance from a foreign authority concerning the temporary removal of electronic data has not yielded a result within thirty days of the issuance of the request by the court, and if a request for legal assistance from a foreign authority for the temporary removal of electronic data would not be expected or would be disproportionately difficult (HPC Article 337 paragraph 1 point 'b' and 'd').

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

There is not any explicit regulation for this situation, thus it is always up to the decision of the investigation authority how to in the concrete case find the location of the server (particularly via legal assistance from the authorities of the possible foreign countries or via EU legal assistance). The procedural regulation can be found in Act CLXXX of 2012 Article 35.

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?*

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

There is not any explicit regulation for this situation, but according to the aim of HPC it must be possible (see question 6, 9, 21).

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?*

It is also possible to do so not just by the court, but also the prosecutor and the investigation authority.

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

No, it is irrelevant.

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, it is always up to the court's opinion to exclude these evidence during the proving process or not (also see question 15). Although the court of appeal has the right to supervise all evidences in their entirety.

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

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

these scenarios are the same, it suffices to only answer the questions once. However, most jurisdictions have different situations in which seizure is possible (e.g. in the context of a search of premises vs. not in the context of a search), so please differentiate between these scenarios, as well and answer the questions for them separately. If you prefer, you can answer the questions in their totality in an integrated explanation, as long as all elements are covered and again, various scenarios are differentiated between.

Please, give as much guidance as possible to enhance our understanding. Always cite the provision of the law or the case law you are relying on (legal basis) and mention conditions, people involved in the action, formal requirements etc., even if not specifically asked.

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

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

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

There is not any general regulation for this situation. It is always up to the cooperation between the investigation authority and the informatician expert during the criminal procedure. Special instructions maybe exist, but those are only relevant in the aspect of the concrete case.

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?*

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

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

There is not any regulation for using mobile forensics and AI technology in criminal procedure yet. Although in 2018 a monograph was published by two prosecutors (Barna Miskolczi, Zoltán Szathmáry), which deals with these issues in detail. They also published a draft for the regulation of AI technology and other instruments of the 21th century's modernization. In 2020 a new committee was established to codify this concept in Hungarian law, but it is still under construction.

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

Answer: Indication of length of answer: couple of paragraphs

According to these criminal offences (eg. child pornography, drug trade, human trafficking, etc.), probably the most important issue is where the criminal offence was committed, thus related to HPC Article 21 paragraph 1 as a main rule those authorities have competence to conduct the criminal procedure where the criminal offence was committed. For example, in case of a fraud committed via the internet with a mobile device, we have to decode where the victim was situated during the conversation with the offender, because this place will determine the competence of the authorities.

During these criminal procedures legal aid is the main method to tackle the multijurisdictional issues.

Of course it is much easier if the forensic examiner is aware of the nature of the crime and the regional laws, but it is not necessary. In practice the authorities (especially investigation authorities and prosecutors) help each other to analyse the differences between the regulation of two (or more) countries.

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

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

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

It is always up to the nature of the concrete criminal offence and other circumstances of the criminal procedure.

According to the legal regulation, HPC Article 394 paragraph 3 point 'c' states that the prosecutor or the investigation authority will suspend the criminal procedure if a request to another country is needed to fulfil a legal aid.

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

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

It is always up to the nature of the concrete criminal offence and other circumstances of the criminal procedure.

The authorities always have the right to decide which instrument seems to be more successful to establish criminal liability.

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

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

According to 2019/1937 Directive of the EU for the protection of whistleblowers, it is getting more and more important to begin a cooperation between criminal investigation authorities and the

private sector. Also a new Ordinance of the Government came into force at the beginning of this year [339/2019. (XII. 23.] which deals with the regulation of compliance for the state owned firms.

Also according to the complaint law of Hungary (CLXV Act of 2013, in force since the 1st of January 2014) if a firm in the private sector detects a criminal offence during the internal investigation it is mandatory to report this to the police.

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)*

There are not any special rules. The participant of the criminal proceedings have the right to ask for their personal data treated confidentially and separately among the files.

- *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)*

These data can be treated separately among the files.

- *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)*

There are not any special rules for these issues.

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

All those information which is important to establish criminal liability, until the termination of criminal proceedings.

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

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

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

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

Section 3: Admissibility of evidence before court

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

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

No, there is not any more.

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

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

The admissibility of evidence collected through mobile forensics are actually the same as for other types of evidence.

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

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

Not following the HPC during the examination of a mobile device can be considered as a relative reason of exclusion as a main rule, thus it is always up to the court in the concrete case to exclude the evidence got that way or not. Thus these evidence should be submitted to the court, except if an absolute reason of exclusion exist (eg. the prosecutor find out before filing the indictment that a member of the investigation authority committed a criminal offence during investigation).

For a detailed answer also see question 15.

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

***41.* Question:** *Specifically, if data in the Cloud is accessed according to criminal procedure, but it turns out to be located outside your jurisdiction does this mean it is not admissible at all? Is it relevant that there was reasonable doubt about the location of the data at the time?*

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

No, this is irrelevant.

In this situation a request for legal aid should be made.

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

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

No, it is always up to the court's opinion to exclude these evidence during the proving process or not (also see question 15).

In general it is always up to the nature of the alteration.

***43.* Question:** *Specifically, are there rules on the used technology, methodology or standard, such as for example that this must be forensically sound as a prerequisite for admissibility? If yes, please elaborate.*

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

No, there are not any special rules.

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

Once in 2000 the Hungarian Supreme Court stated that video recording with a hidden camera can be used as evidence during the proving procedure (EBH 2000. 296.).

Since then I could not find any new decision related to mobile devices and criminal prodecure among the published decisions of the Supreme Court.

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

No, as it have been discussed previously, it is mostly up to the court's decision in the concrete case.

***46.* Question:** *Is a failure to comply with Data Protection law, or privacy rules in itself, enough to refuse admissibility of the evidence, even when procedure is otherwise followed?*

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

No, but there could be other consequences of the failure (eg. the court can report the breach of law to the competence authority).

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

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

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

No, I could not find any cases in Hungarian criminal practice in these issues, at least considering the legally finished cases.

As mentioned earlier, I was unable to access any case law regarding the role of mobile phones in the criminal procedure; the common aspects of the role of the mobile phones was the determination of the location of an offender based on cell information, furthermore, phone conversations can be tapped - the latter requiring a court order. (see section 231 of the HPC)

However, we could recall an interesting case, although it has to be emphasized that it is still in the first instance, therefore the decision is not final. In this case, the offender is charged with 'Causing a Road Accident' (section 235 of the HCC). According to the bill of indictment, the offender used his frontal camera on his iPhone to video himself while driving way over the speed limit in downtown Budapest, causing an accident resulting in two fatalities and more injuries. This video was played during the trial, and - as the case gained nationwide notoriety - the press could tape this part of the trial (the face of the offender is covered in the video as he did not consent to release his image). Furthermore, this video was used by the vehicular expert to determine the possible speed of the offender based on the distance and time shown in the video. The defence counsel filed a motion to exclude this opinion claiming that the expert does not have the required informatician qualification. As the first instance court is predicted to decide the case this year, the final sentence should not be expected earlier than 2021-22. The video can be accessed here: https://www.youtube.com/watch?v=ca12uowxzVQ

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?*

  No, it is not.

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

- *Are there rules on how to interpret mobile forensic evidence or requirements which must be complied with for the evidence to be considered reliable?*
  No, there are not.
- *Must such evidence be examined by an expert witness?*
  It is not obligatory, but the common practice.
- *If not obligatory, is this a common practice?*
  See the answer on the previous question.
- *What are the requirements for experts (experience, independence, training, etc.)?*
  Mostly at least a BA degree in informatician sciences and it is also mandatory to be a member of forensic expert's register.
- *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?*
  All the forensic expert have to be a member of the Hungarian Chamber of Forensic Experts. It has a separated section for informatician experts.

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

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

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

See question 44.

***50.* Question:** *Is there in your jurisdiction an established and recognised standardisation(s) of the processes of collection, analysis, interpretation and reporting of digital evidence that must be followed for the interpretation and presentation of evidence before a court? Or alternatively*

which is not obligatory but considered as critical for the validity of evidence, its quality or the impact of the evidence and its acceptance by the courts? If yes, please elaborate.

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

No, the Hungarian regulation of criminal proceedings is based on the principle of free evaluation of evidence and it is also valid for the collection, analysis, etc. of digital evidence. Also there is not any pre-set quality and impact of the evidence, it is always up to the discretion of the court.

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

No, I could not find these kind of decisions.

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.

There is not any special rules or guidance for these issues in Hungary. The most common way to respect the right to a fail trail could be to respect the personal life of the perpetrator. Thus, if for example the suspicion is that the offender keeps child pornography on his mobile device, then it would not be necessary to read all of his/her personal correspondence, etc.

Also if the seizure is not necessary any more and this is not likely that a confiscation will be imposed, then the seizure should be terminated.

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

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

No, it is not yet, but there are opinions in criminal practice that is should be.

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

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

No, there is not. If an expert undertakes the task, he/she has to finish the opinion usually in 60 or 90 days.

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

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

The prosecutor shall act as the public accuser. The prosecutor shall be obliged to consider both the circumstances aggravating and extenuating for the defendant and the circumstances aggravating and mitigating the criminal liability in all phases of the proceedings. The prosecutor

a) may order an investigation, assign the investigating authority to conduct the investigation, and may instruct the investigating authority to perform – within the its own geographical jurisdiction – further investigative actions or further investigation, or to conclude the investigation within the deadline designated by the prosecutor,

b) may be present at the investigative actions, and may examine or send for the documents produced during the investigation,

c) may amend or repeal the decision of the investigating authority, and shall consider the complaints received against the decision of the investigating authority,

d) may reject the denunciation, terminate the investigation and order the investigating authority to terminate the investigation,

e) may take over the proceedings (HPC Article 26).

The court shall be responsible for the administration of justice.

As a main rule courts shall be responsible for making a decision on controlling or depriving somebody of his or her liberty.

Prior to the indictment the tasks of the court shall be performed by the investigating magistrate (HPC Article 11).

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

The defendant is the person against whom criminal proceedings have been instituted.

The defendant shall have the right to defence.

Everyone has the right to defend himself/herself at liberty. This right may only be restricted as well as a person may be deprived of his freedom only for the reason and only in virtue of the procedure allotted in HPC.

The defendant may undertake his/her own defence, and may be defended by a counsel at any phase of the proceedings. The court, the prosecutor and the investigating authority shall ensure that the person against whom criminal proceedings are conducted can defend himself/herself as prescribed in HPC.

The defendant is entitled to

a) receive information on the suspicion, on the charge and any changes therein,

b) – unless provided otherwise by HPC – be present at the procedural actions, and inspect the documents affecting him or her in the course of the procedure,

c) be granted sufficient time and opportunity for preparing his or her defence,

d) present facts to his or her defence at any stage of the procedure, and to make motions and objections,

e) file for legal remedy,

f) receive information from the prosecutor and the investigating authority concerning his or her rights and obligations during the criminal proceedings (HPC Article 39).

Those persons may be heard as a witness who may have knowledge of the fact to be proven.

Unless an exemption is provided for in HPC, anyone summoned as a witness shall give testimony.

At the request of the witness, the acting court, prosecutor or investigating authority shall establish and refund the cost – to the extent specified in a separate legal regulation – incurred in connection

with the appearance of the witness. The witness shall be advised of this in the subpoena and at the time of the conclusion of the examination (HPC Article 168).

The victim is the party who's right or lawful interest has been violated or jeopardised by the criminal offence.

The victim shall be entitled to

a) be present at the procedural actions (unless provided otherwise HPC) and to inspect the documents affecting him or her in the course of the procedure,

b) make motions and objections at any stage of the procedure,

c) receive information from the court, the prosecutor and the investigating authority concerning his or her rights and obligations during the criminal proceedings,

d) file for legal remedy in the cases specified in HPC (HPC Article 50).

5.1 The Prosecution

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

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

All prosecutor have to obtain 50 points in every 5 years during the prosecutor's education system. To receive these point they usually have to visit conferences which are usually deal with the 21st century's modern devices. It is also quite common that prosecutors receive a second degree in for instance criminalistics.

Although a concrete guidance is not known yet in this field.

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

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: Indication of length of answer: couple of paragraphs.

As a main rule no, in Hungary judicial control is only needed during investigation, if the personal freedom of the offender should be limited. The exception is during covert intelligence gathering, which usually needs a permission by court.

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

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

There is no significant difference compare to other kind of evidence, thus it is not possible to give a specified answer.

5.3 The defendant and defender

***59.* Question:** *Are there rules and standards regulating the defendant and his/her defender's rights to access and to make copies of the acquired mobile evidence? Are they able to get any information on the process used to acquire mobile forensic evidence (e.g. information on how the tools work, the procedures used, the parties involved and how the validity of the results is guaranteed)? Please refer to case law if possible.*

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

HPC Article 160 states that the detailed rules for these issues can be found in a separated act. This act is the 12/2018. (VI 12.) Ordinance of the Department of Justice. Article 22 of this Ordinance states that during the examination of the file, the person entitled to inspect it may use the technical means at his disposal, in particular a camera, camcorder, handheld scanner, mobile device, to make a copy or record of the file. pre-trial and the trial phase of the criminal proceedings. Article 27 of this Ordinance states furthermore that the court, the public prosecutor's office and the investigating authority may also provide access to the file by electronic access to the file, in particular through a dedicated web interface, provided that the necessary technical conditions are in place.

5.4 Witnesses

60. **Question:** *During the pre-trial stage, how is the right to privacy of the witnesses preserved? Are there any practical steps taken to exclude certain types of information which are cumulatively non-relevant to the case and too private? Are there particular requirements for witnesses regarding their capability to testify in terms of mobile forensics both in the pre-trial and the trial phase of the criminal proceedings? Please refer to case law if possible.*

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

The court, the prosecutor and the investigating authority may order ex officio or upon the request of the witness or the legal counsel acting upon the behalf of the witness that the personal data of the witness shall be treated confidentially and separately among the files. In such cases the confidentially treated data of the witness may be examined only by the court, prosecutor and investigating authority proceeding in the case (HPC Article 99).

There is not any known case law, probably because these issues are strongly related to the investigation itself.

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

5.5 The Victim

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

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

The victim shall be entitled to

a) be present at the procedural actions and to inspect the documents affecting him or her in the course of the procedure,

b) make motions and objections at any stage of the procedure,

c) receive information from the court, the prosecutor and the investigating authority concerning his or her rights and obligations during the criminal proceedings,

d) file for legal remedy in the cases specified in this Act (HPC Article 51).

The court, the prosecutor and the investigating authority may order ex officio or upon the request of the victim or the legal counsel acting upon the behalf of the victim that the personal data of the victim shall be treated confidentially and separately among the files. In such cases the confidentially treated data of the victim may be examined only by the court, prosecutor and investigating authority proceeding in the case (HPC Article 99).

Evidence obtained via mobile forensics can be used, but it always up to the court's decision to consider the value of these evidence.

Section 6: Comments

If you feel some important elements of your national law relating to the use of mobile forensics in criminal investigations have not sufficiently been covered, please explain them here. If you feel an overview is missing, please also provide guidance on this below.

Answer: Indication of length of answer: few paragraphs up to a couple of pages.

-