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: Vojčík & Partners (law firm), my position is Managing Partner

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

Answer: Košice, Slovak Republic

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: No, it is a "thing", an "item" in general under Section 130 Act No. 300/2005 Coll. Criminal Code as amended (hereinafter referred to as the "**Criminal Code**").

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?*

   An option previous to the seizure of thing is surrendering an item under Section 89 of Act No. 301/2005 Coll. Criminal Procedure as amended (hereinafter referred to as the "**Criminal Procedure**"). Under Section 89 par. 1 of the Criminal Procedure "*Any person having on him an item relevant to the criminal proceedings shall have the duty to present it upon request to a police officer, a prosecutor or the court; if the item is to be seized for criminal proceedings purposes, he shall have the duty to surrender it to the aforesaid bodies upon request*."

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?*

   Yes, there are limitations. Meaning, the fundamental rights and basic limits of private life, personal data, professional confidentiality must be out of the picture if not directly connected to the investigated crime or other exceptions (e. g. a person is freed from confidentiality obligations). General provision is that an item relevant to the criminal proceedings (e. g. communication with the victim).

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

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

Yes, it is if the device is in possession of the competent authorities legally. However, recent cases showed that this is not always successful and in one case, authorities did posses the device, but were not able to breach its protection.

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

   Yes, Section 90 par. 1 of the Criminal Procedure states *"If the storage of the stored computer data is necessary for the clarification of the facts necessary for the criminal proceedings, including operating data that is stored through a computer system, the presiding judge and, prior to the commencement of criminal prosecution or in pre-trial proceedings the prosecutor may issue an order based on circumstantial reasons to the person who has possession of or control over such data, or to the provider of such services, requesting them to a) store such data and maintain the integrity thereof, b) allow the production or retention of a copy of such data, c) prevent access to such data, d) remove such data from the computer system, e) surrender such data for the purposes of criminal proceedings.*"

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

   Person in possession may surrender the item in question voluntarily under Section 89 of the Criminal Procedure. If not, he or she must act in accordance with an order to store and/or disclose computer data under Section 90 of the Criminal Procedure or authorities might also seize the device itself as a thing under Section 91 of the Criminal Procedure; depending whether authorities are interested in data send from or to the device or device and its content.

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

   No. Also, if the person in possession is the defendant, it would be against the prohibition of self-incrimination.

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

    Yes, authorities must provide him or her with an order explaining what the purpose of their acts is and what is it related to.

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

    Home search warrant may be issued by presiding of a panel and, in pre-trial proceedings, by a judge for pre-trial proceedings on a motion from a prosecutor. The warrant to conduct the

search of a person shall be issued by the presiding judge of a panel or, in pre-trial proceedings, by a prosecutor; or, with the authorisation by the latter, it may be issued by a police officer.

Formal requirements are the reasons which led to the issuance of the warrant, including the mention of things or persons, which should be found (searched) during the inspection, as well as the justification, from which the facts justifying the interference with the freedoms protected by the Slovak Constitution are clear and the Convention for the Protection of Human Rights and Fundamental Freedoms.

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

No, Criminal Procedure states *"Any person having on him an item relevant to the criminal proceedings shall have the duty to present it upon request to a police officer, a prosecutor or the court"*

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.*

This will be similar to finding out the content of e-mail communication (in terms of possible use of the order under Section 116 para. 6 of the Criminal Procedure "*In criminal proceedings for an intentional criminal offence for which this Act sets out a prison sentence with an upper penalty limit of at least three years, for a criminal offence of the protection of privacy in the dwelling under Section 194a, fraud under Section 221, dangerous threats under Section 360, stalking under Section 360a, spread of alarming news under Section 361, incitement under Section 337, endorsement of a criminal offence under Section 338, for a criminal offence by which grievous bodily harm or death was caused or for another intentional criminal offence, the conduct of which is bound by an international treaty, a warrant for the determination and notification of data on telecommunication operations, which is subject to telecommunications privacy, or subject to personal data protection, which is necessary to clarify the facts relevant to the criminal proceedings, may be issued. The warrant may be issued if the purpose pursued*

may not be attained otherwise or if its attainment in another manner would be considerably hindered.", also in cases where data important for criminal proceedings will be located on different web repositories. This allows to obtain data transmitted through a computer system, i. e. also content data that is transmitted via a computer network between computers, or data that "remains" stored within the computer network on the server of the email service provider (email communication, etc.). The essence of the order according to Section § 116 par. 6 of the Criminal Procedure there will therefore be a court order to law enforcement authorities to break into a specific email box, find out its contents and secure (download) the content that is relevant to the criminal proceedings (for example, invoice, contract, conversation between the accountant and the suspect, etc.).

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

Only in Section 116 para. 1of the Criminal Procedure.

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.*

Yes. Illegal evidence must not be admitted.

Mobile device seized

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

Yes, under Section 91 of the Criminal Procedure *"If a thing relevant for criminal proceedings or computer data are not surrendered upon request by the person who have it in his possession, they may be withdrawn from that person upon an order of the presiding judge of a panel or, in pre-trail proceedings, upon an order of a prosecutor or a police officer. Police officers may issue such order only with prior consent of a prosecutor*."

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

Stated in the previous answer.

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

Depending of what is the interest of the authorities with regards to the criminal proceedings and what is covered by the order, if computer data or the device itself as a thing; depending whether authorities are interested in data send from or to the device or device and its content.

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?*

Yes, there are limitations, however their limitations are not stated rigidly and are always up for interpretation (e. g..”private life” differs in case of drug trafficking and child abuse). As everywhere else, the fundamental rights and basic limits of private life, personal data, professional confidentiality must be out of the picture if not directly connected to the investigated crime or other exceptions (e. g. a person is freed from confidentiality obligations). General provision is that an item relevant to the criminal proceedings (e. g. communication with the victim).

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

Yes, if the person surrenders the device under Section 89 of the Criminal Procedure. Only after not providing this voluntarily, seizure may be used and as mentioned earlier, in one case before the Slovak Constitutional Court (docket no.: II. ÚS 78/2019-55), the technicians were not able to breach the protection.

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

No. Also, if the person in possession is the defendant, it would be against the prohibition of self-incrimination

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

Yes, he or she must be informed about reasons which led to the issuance of the order, including the mention what information or evidence might be found (e. g. what data, what scope, what form and content), as well as the justification, from which the facts justifying the interference

with the freedoms protected by the Slovak Constitution are clear and the Convention for the Protection of Human Rights and Fundamental Freedoms.

23. *Is it allowed to use technical tools to bypass security measures and/or anti-forensic measures?*
Yes. Currently there is a very important ongoing case in Slovak Republic in which the encryption might have been broken. However, it's a live case, thus should not be further discussed.

24. *Does it matter whether this person is the accused or witness/third party or the victim?*
Only regarding the self-incrimination.

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.*

26. This will be similar to finding out the content of e-mail communication (in terms of possible use of the order under Section 116 para. 6 of the Criminal Procedure "*In criminal proceedings for an intentional criminal offence for which this Act sets out a prison sentence with an upper penalty limit of at least three years, for a criminal offence of the protection of privacy in the dwelling under Section 194a, fraud under Section 221, dangerous threats under Section 360, stalking under Section 360a, spread of alarming news under Section 361, incitement under Section 337, endorsement of a criminal offence under Section 338, for a criminal offence by which grievous bodily harm or death was caused or for another intentional criminal offence, the conduct of which is bound by an international treaty, a warrant for the determination and notification of data on telecommunication operations, which is subject to telecommunications privacy, or subject to personal data protection, which is necessary to clarify the facts relevant to the criminal proceedings, may be issued. The warrant may be issued if the purpose pursued may not be attained otherwise or if its attainment in another manner would be considerably hindered*.", also in cases where data important for criminal proceedings will be located on different web repositories. This allows to obtain data transmitted through a computer system, i. e. also content data that is transmitted via a computer network between computers, or data

that "remains" stored within the computer network on the server of the email service provider (email communication, etc.). The essence of the order according to Section § 116 par. 6 of the Criminal Procedure there will therefore be a court order to law enforcement authorities to break into a specific email box, find out its contents and secure (download) the content that is relevant to the criminal proceedings (for example, invoice, contract, conversation between the accountant and the suspect, etc.).

27. *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?*

Under the principle of officiality which is binding for Slovak criminal law, it is up to authorities to exercise the rights granted to them and investigate reported crimes. We are not privy to their internal proceedings.

28. *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?*

No and to our knowledge, this presents practical difficulties.

29. *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 necessary to mention that the service provider (e. g. operator of email services) can be requested in accordance with Section 116 para. 2 of the Criminal Procedure only to provide traffic data, such as IP address (finding the user who had a specific IP address at the time), finding the password (access) to the e-mail box and the like, but in no case can the content of the e-mail communication be secured from the service provider. In other cases there will be a court order to law enforcement authorities to break into a specific email box, find out its contents and secure (download) the content that is relevant to the criminal proceedings.

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

Only in Section 116 para. 1of the Criminal Procedure.

31. *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*

Yes. Illegal evidence must not be admitted.

Please, answer all these questions separately for each scenario or instance which, in your opinion, is (partially) subject to different rules than other scenarios. At least, make the difference between the scenarios where a mobile device is seized and where it is not. If all sub-scenarios in one of these scenarios are the same, it suffices to only answer the questions once. However, most jurisdictions have different situations in which seizure is possible (e.g. in the context of a search of premises vs. not in the context of a search), so please differentiate between these scenarios, as well and answer the questions for them separately. If you prefer, you can answer the questions in their totality in an integrated explanation, as long as all elements are covered and again, various scenarios are differentiated between.

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

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

32. **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: The essential fact of securing the evidence in question against unauthorized manipulation by third parties. Protection against possible interference from the "outside" is realized usually by sealing the evidence. This is a procedure where everyone the entrances, exits and potentially openable or removable parts of the evidence shall be sealed in such a way that intervention in these parts was obvious that they were affected. Expert or authorities after examination evidence, he is

obliged to reseal this evidence and return it to authorities or another relevant person so that if it is necessary to re-examine or verify the evidence, there is no doubt that that the evidence has not been tampered with. The evidence must remain as follows until the evidence is returned or the criminal proceedings are terminated.

Under Section 58 of the Criminal Procedure there shall be minutes about each act of criminal proceedings, usually at the time of the act or immediately thereafter. It is about stabilizing events, criminal proceedings so that it is possible to place documented acts in writing in the file, re-evaluate them course, as well as legality. Compliance of the minutes with the facts and the requirements of the law on conditions its implementation can become an important incentive to examine the legality of criminal proceedings.

Computer data can become legal evidence only if it meets the condition of authenticity, originality, credibility and has been obtained in a lawful manner.

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: To our knowledge, there are none, however, there might be internal norms or guidelines for the authorities.

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 main issue might be cloud related crimes as their true operators might be lost on the Internet and hide their traces. We do not believe that forensic expert should be aware of legal

aspects as he only provides technical way towards conducting investigation and gathering evidence.

***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:

***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.

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

Answer: Only in providing protection for data, not the other way around**.**

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

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

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

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

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

Answer:. Computer data can become legal evidence only if it meets the condition of authenticity, originality, credibility, authenticity and has been obtained in a lawful manner.

Authenticity of computer data

In general, authenticity is a property that ensures that the identity of an entity or source is such that for which it is issued. In our context, this means that the authenticity of computer data represents its identity with computer data that has been created, recorded and stored. In addition,

in order to mark a computer data as authentic, we need to resolve the question of its originality, authenticity and authenticity.

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

Originality

Originality means that the computer data is in the state in which it was at the material time and has not been affected in any way. When proving interference with computer data, proving its damage, modification, destruction of even a small part is possible o non-original evidence, the further examination and subsequent evidentiary use of which is without legal basis meaning. Detection of computer data is always irrefutable evidence because it is not possible to determine its original condition by examination. An expert in the performance of his expert activities it can only work with verifiable evidence. This postulate forms the basis of his research and the expert activity itself.

Truthfulness

The truthfulness of the computer data is confirmed if it has been established that it has not been tampered with before examination. Truthfulness means that evidence has not been modified before it was examined and that it was created by the original process without deliberate involvement of one of the parties to the proceedings in the taking of evidence. False evidence is like evidence inadmissible in criminal proceedings. It is the expert's duty to deal with the truthfulness of the evidence rather than on it shall commence any further expert examination. In the event of a reasonable doubt as to the truthfulness of the evidence, further examination must be suspended until the doubt is rebutted. When examining the truthfulness of the computer data, the expert finds out whether there was any evidence affected before its examination.

Credibility

The plausibility of evidence and at the same time computer data must be assessed from several views. One of them is the legality of obtaining it. As mentioned above, credible evidence can be considered only such evidence that has been obtained in a manner prescribed by law, compliance with procedural procedures and the relevant provisions of the Criminal Procedure. If, for example

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

the carrier with computer data is handed over to authorities by the injured party, who claims that he obtained this data from the computer of the defendant in his absence and did so because he is suspected of having committed a criminal offense cannot be credible evidence because it was obtained illegally. In addition, in the given case, it may be a person who has the motive to provide authorities with purposeful evidence directed against the defendant.

Regarding the data privacy, Section 3 par. 3 of act no. 18/2018 Coll. on protection of personal data as amended states "*This Act applies to the processing of personal data by the Police Force, the Military Police, the Prison and Judicial Guard Corps, the Financial Administration, the Prosecutor's Office and the Courts (hereinafter referred to as the "Competent Authority") for the purposes of crime prevention, detection, criminal prosecution and criminal prosecution. or for the purpose of enforcement of decisions in criminal proceedings, including protection against and prevention of threats to public order (hereinafter referred to as "performance of tasks for the purposes of criminal proceedings")*". Since the stated act is almost identical to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), it is a standard personal data processing by a state authority.

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: The area of protection of the privacy of individuals and the interest of the state against eavesdropping and misuse of information is included in Act no. 166/2003 Coll. on the protection of privacy against unauthorized use of information and technical means and on the amendment of certain laws (the Act on protection against interception) as amended no. 652/2004 Coll. (indirectly), 757/2004 Coll., 311/2005 Coll., 59/2009 Coll., 290/2009 Coll., 291/2009 Coll., 547/2010 Coll. ., 404/2015 Coll. Paradoxically, this law lays down the conditions for the use of information technology (wiretaps, audio or video recordings) in addition to its title without the prior consent of the person who is invaded by the authority of the state that uses the information technology.

The said Act does not apply to the use of information and technical means in criminal proceedings under a special law on Criminal Procedure. Information and technical means may be used only with the written consent of the legal judge only for the necessary time, but for a maximum of six months. During the use of information technology, the state authority is obliged to constantly examine whether the reasons for their use persist. If these reasons have passed, he is obliged to stop the use of information technology immediately.

The state authority is obliged to inform the legal judge about the termination of the use of information and technical means pursuant to paragraph 1.The use of information technology is a process of secrecy, the results of which can be used as evidence in criminal proceedings if they contain information that a criminal offense has been committed.

The area of securing information in criminal proceedings is regulated by the Criminal Procedure Code in Title V in the provisions of Section 113 et seq., Specifically electronic evidence in Section 115 on interception and recording of telecommunications traffic and Section 116 on notification of telecommunications traffic data - data on mobile devices from calls, sms, etc.The order for interception and recording of telecommunication traffic is issued by the chairman of the court senate, before the commencement of criminal prosecution and in the preparatory proceedings by the judge for the preparatory proceedings on the proposal of the prosecutor. A similar procedure on the part of the court is also in obtaining consent to interception and recording of telecommunications traffic, obtaining data from mobile devices, which is limited by exhaustively listed intentional crimes, with the upper limit of imprisonment penalty of at least three years.

In order to compare data in information systems, it is possible to compare data in information systems pursuant to the provisions of Section 118 of the Criminal Procedure Code on the basis of

an order from the chairman of the court senate and before the commencement of criminal proceedings or in the preparatory proceedings of the prosecutor.

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

Answer: The criteria for the admissibility of evidence gathered through forensic analysis are clearly more rigorous and strict in comparison with other evidence, and any errors in obtaining them result in their illegality and inapplicability as evidence in criminal proceedings.

The area of use of illegally obtained evidence and its inapplicability in criminal proceedings is dealt with in expert literature and it is addressed by the relatively extensive case law of the courts of the Slovak Republic, the Supreme Court of the Slovak Republic and the Constitutional Court of the Slovak Republic.

***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: Legislatively, the principle of formalism is preferred in the Criminal Procedure Code of the Slovak Republic. Compliance with legal procedural rules is preferred and takes precedence over the interest of the criminal justice system in obtaining recognition of the guilt of the accused for an act committed. Evidence thus obtained illegally, which cannot be used in criminal proceedings, is ultimately assessed in relation to the accused (defendant) in his favor, also with reference to the principle in *dubio pro reo* (in case of doubt in favor of the accused).

In practice, the most common are the so-called private recordings submitted by the parties to criminal proceedings for use as evidence. It is an embodiment of e.g. photographs, video recordings of another person, or their expressions via a mobile phone, camera or camera system.

On the question of their procedural (in) applicability in criminal proceedings, we come across the provision of § 119 par. 2 of the Criminal Procedure Code as well as the provisions of § 12 of the Civil Code.

The recording of another person without his/her consent comes into conflict with the provisions of § 12 of the Civil Code, because without his/her consent it is always an interference with the right

to protection of the personality of the person whose film or recording is made, e.g. targeted photography of another person on the street without the consent of the photographed person.

***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: This area is currently strongly resonating in the Slovak Republic, mostly with a reference to the ongoing criminal trial of the murder of a journalist and his fiancée, where calls and text messages play an important role (Threema application).

In such cases, it is a sovereign question for the court to assess the admissibility and applicability of the data in the cloud, which, if in the private regime, is subject to the above principles of lawfulness in obtaining them. The situation is different if the data is in public mode, which may not be secured and can be accessed via social networks and Google. Of course, even if there are doubts about the location of the data in such a case, these should be dispelled or removed so that they can be used in criminal proceedings as evidence.

Similarly, if doubts about the location of data could not be removed, a situation of their inapplicability in criminal proceedings would arise as evidence.

***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: If the evidence in the form of mobile data was obtained lawfully and would therefore be usable as evidence in criminal proceedings, then the question of their possible changes would be for a technical expert to answer, to what extent the original data was compromised in such a way as to clarify their applicability and thus legalize it. Of course, in the end, it will be up to the court (judge) to decide in a comprehensive assessment.

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

***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: In the Slovak Republic, no specific rules have been set regarding the technology, methodology or standards used in this area. The question of their reliability and applicability is in the pre-trial proceedings of law enforcement bodies, which are the police and the prosecutor's office, which supervises compliance with the law before prosecution and in pre-trial proceedings.

***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: Yes.

• Collection of Opinions and Decisions of the Supreme Court of the Slovak Republic R 38/2003

• Collection of Opinions and Decisions of the Supreme Court of the Slovak Republic R 45/2018

• Judgment of the Criminal Law Collegium County Court in Žilina of 14 September 2010, file no. 1 To 42/2010

• Resolution of the Supreme Court of the Slovak Republic of 21 September 2011, file no. 3 To 2/2011

• Judgment of the Supreme Court of the Slovak Republic of 28 May 2013, file no. 2 Tdo 24/2013

• Resolution of the Supreme Court of the Slovak Republic of 13 March 2018, file no. 4 To / 12/2015

• Resolution of the Supreme Court of the Slovak Republic of 23 March 2017 file no. 5 Tdo 7/2017

• Resolution of the Supreme Court of the Slovak Republic of 16 April 2018, file no. 5 To 6/2017

***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: In the Slovak Republic, there is no standardization in court practice of the processes of collecting, analyzing, interpreting and communicating digital evidence that must be followed in order for evidence to be admissible.

***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: The legal regulation of personal data protection or privacy rules regulated by Act no. 18/2018 Coll. on the protection of personal data and on the amendment of certain laws as amended no. 35/2019 Coll. (indirectly) no. 221/2019 Coll. (GDPR Act) does not regulate the area of assessing the admissibility of evidence.

Consequences of non-compliance with legal regulations on personal data protection or privacy protection rules are addressed by the GDPR Act as administrative offenses with the possibility of imposing a disciplinary fine.

***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:

• Judgment of the Supreme Court of the Slovak Republic of 28 May 2013, file no. 2 Tdo 24/2013

In the given case, the Regional/County Court in Banská Bystrica recognized as legally performed evidence - reading a record from the telecommunication operation of a mobile operation - in a foreign language, while the Supreme Court of the Slovak Republic ruled in an appeal procedure as an extraordinary remedy as follows:

"*If under the procedure of § 115 Penal Code a communication in a foreign language is recorded, a condition for the use of a record of telecommunication traffic in the sense of § 115 as (original) evidence is its literal transcript in a foreign language, translated into Slovak, if the prepared record allows it and the interpretation of the entire content or the relevant part of the content of the record translated into Slovak and its transcription into text form.*"

In the statement of reasons, it stated, inter alia, that the illegality of the proof of telecommunication traffic recording was relative. As part of the evidence, the search for evidence - a record of

telecommunications traffic - was carried out in a lawful manner. The making of a transcript of a record for the absence of a legal procedure for translating from a foreign language and the literal nature of the transcript of legality contradicts, which means that the other stages of the court-taking evidence and evaluating the evidence become null and void.

• Resolution of the General Prosecutor's Office of the Slovak Republic of 24 June 2014, file no. no. VII / 1 Gv 101/2012

In that case, there was a situation where wiretaps ordered and executed in criminal proceedings involving persons other than those in the present case were used as evidence in the preparatory proceedings. After evaluating the lawfulness of the evidence performed in the preparatory proceedings, the prosecutor decided that the evidence thus obtained, even if obtained in a lawful manner in another case, is inapplicable in the given criminal case and therefore criminal prosecution under Section 215 of the Criminal Procedure Code.

- Judgment of the Constitutional Court of the Slovak Republic of 29 April 2015, file no. PL. ÚS 10/2014

The above-mentioned finding of the Constitutional Court of the Slovak Republic was published in the Collection of Laws under no. 139/2015 Coll., by which the Constitutional Court of the Slovak Republic ruled that the provisions of § 58 par. 5 to 7 and § 63 par. 6 of Act no. 351/2011 Coll. on electronic communications as amended, § 116 of Act no. 301/2005 Coll. Criminal Procedure Code as amended and § 76a par. 3 of the Act of the National Council of the Slovak Republic no. 171/1993 Coll. on the Police Force, as amended, **are not in accordance** with Art. 13 par. 4, Art. 16 par. 1, Art. 19 par. 2 and 3 and Art. 22 of the Constitution of the Slovak Republic, Art. 7 par. 1, Art. 10 par. 2 and 3 and Art. 13 Charter of Fundamental Rights and Freedoms and Art. 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

In the above-mentioned judgment, the Constitutional Court resolved the non-compliance of the provisions of the laws with the Constitution of the Slovak Republic in the area of reporting data on telecommunications traffic in criminal proceedings under §116 of the Criminal Procedure Code by issuing a judge's order and in the prosecutor's preparatory proceedings to seize and report telecommunications traffic data.

The contested provisions of the Criminal Procedure Code entitle law enforcement authorities to obtain from the providers of electronic communications for the purpose of clarifying the facts relevant to the criminal proceedings data on the telecommunications traffic that is otherwise subject to telecommunications secrecy or to which the protection of personal data applies. The challenged provisions of the Police Force Act entitle the Police Force, for the purposes of detecting and

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

documenting criminal activity, to the extent necessary to perform a specific task of the Police Force and for the time necessary to fulfill this task to request data from electronic communications providers in a way that allows remote, continuous and direct access.

Access by public authorities to this data without the consent of the users of these services directly and appreciably affects their right to privacy in the form of the right to informational self-determination, given the possibility of deriving information about the place, time and participants in the communication, as well as the way they communicate, because to that extent it deprives them of the opportunity to decide for themselves whether to make this information available to other persons.

The power of law enforcement authorities to require the establishment and communication of data on the traffic carried out cannot be regarded as a normal or routine means of preventing and detecting crime, given the intensity of its interference with this fundamental right. These means of combating crime can only be used if there is no other and more friendly means of achieving this objective.

The criterion of proportionality of the intervention means maintaining a balance in the relationship between the individual's right to privacy and the choice of the means available to the State in pursuit of a legitimate aim. Their choice is limited by the fact that interference with the right to privacy is possible only when necessary and can only be done in the spirit of the demands placed on a democratic society.

In this regard, the Constitutional Court of the Slovak Republic stated that the legality of state intervention in the right to privacy means that interference is possible only on the basis of law, resp. of the valid legal regulation, while the assessment of the fulfillment of this condition is based on whether the availability and predictability of the law has been respected.

At present, the already alleged non-compliance of the above provisions of legal regulations has been eliminated by the adoption of such legal provisions which are in accordance with the Constitution of the Slovak Republic.

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

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

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

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

Answer: In Slovakia, criminal law in general is well established and given that everything that can contribute to the proper clarification of the matter and what was obtained from the means of evidence under this Act or under a special law can serve as evidence. The means of evidence are, in particular, the examination of the accused, witnesses, experts, opinions and expert opinions, verification of the on-site statement, recognition, reconstruction, investigation, inspection, cases and documents important for criminal proceedings, notification, information obtained using information or operational means -finding activities (§ 119 para. 2 of the Criminal Procedure Code).

With reference to those mentioned in the criminal proceedings, there are no general rules or guidelines on the interpretation and presentation of evidence from a mobile phone, and evidence from a mobile phone has the same value as other secured evidence. In other words, evidence from a mobile phone has no advantage or higher value of evidence than other evidence and, if necessary, can be examined by experts, but only in the technical field.

There is no centralized management of mobile forensic operations in the Slovak jurisdiction and evidence in this area is provided by law enforcement authorities and the prosecutor submits a charge to the court in accordance with the relevant provisions of the Criminal Procedure Code.

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

***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: The interpretation and presentation of evidence generated by mobile forensics is subject to the relevant provisions of the Criminal Procedure Code and the taking of evidence that does not contain a specific procedure in this area.

In this direction, there was a case law regulating the preparation of transcripts and the presentation of recorded telecommunications communication in a foreign language (Judgment of the Supreme Court of the Slovak Republic of 28 May 2013, file no. 2 Tdo 24/2013), according to which if under the procedure under § 115 of the Penal Code communication in a foreign language is recorded, a condition for the use of such record as evidence, is its literal transcript and translation into Slovak language.

As mentioned above, the recording of telecommunications traffic is evidence like any other evidence that is presented on the relevant technical sound equipment, respectively, video-audio equipment.

***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: There is no standardization in the Slovak jurisdiction of the processes of collecting, analyzing, interpreting, and reporting digital evidence, which must be followed when interpreting and presenting evidence in court.

We refer to the general provisions on evidence in criminal proceedings, the provision of § 119 para. 2 of the Criminal Procedure Code, according to which all that can contribute to the proper clarification of the matter and what was obtained from the means of evidence under this Act or under a special law may serve as evidence.

The analysis, interpretation and communication of digital evidence shall be carried out in accordance with the above general principles.

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

The Criminal Procedure Code specifically regulates the following evidence_

- Documentary and factual evidence (§ 153)
- Inspection (§ 154)
- Examination of the body and similar acts (§ 155)
- Examination and autopsy of the corpse and its exhumation (§ 156)
- Investigation experiment (§ 157)
- Verification of the testimony at the crime scene (§ 158)
- Reconstruction (§ 159)
- Voice test and voice sample (§ 160)

***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: In the published case law, we see one case in which the issue of legal procedure and applicability of evidence from the mobile forensic system was addressed, which is listed in the answer to question 49 of this questionnaire. (Judgment of the Supreme Court of the Slovak Republic of 28 May 2013, file no. no. 2 Tdo 24/2013).

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: The Slovak legal system regulates the right to a fair trial, which is enshrined in the Constitution of the Slovak Republic Art. 46 par. 1 according to Art. 6 of the Convention for the Protection of Human Rights and Freedoms.

There is no special case law on how to respect the right to a fair trial in cases obtained through the mobile forensic system. This right is generally referred to in the current case law in various criminal cases, in particular not only in the field of obtaining and applying evidence obtained by means of a mobile phone.

Likewise, the principle of equality of arms is applied in practice in that a party has a reasonable opportunity to submit its submissions on terms which are not significantly less favorable than those available to the other party.

The principle of equality of arms as one of the elements of the broader concept of due process requires that each participant be given a reasonable opportunity to present his or her case under conditions which do not place him/her at an obvious disadvantage to his/her counterparty. In addition to this requirement, the concept of a fair trial includes the right to an adversarial procedure, according to which participants must not only be acquainted with the evidence necessary for their proposal to be successful, but must also be aware of and comment on all evidence and opinions submitted for the purpose of influencing a court decision.

(see Judgment of the Constitutional Court of the Slovak Republic file no. II. ÚS 249/2012 of 18 April 2013)

Ultimately, this principle (principle) is expressed in the Criminal Procedure Code in the principle of adversarial proceedings, which is guaranteed by many international treaties on human rights and freedoms, which are in accordance with Art. 7 par. 5 and Art. 154c of the Constitution of the Slovak Republic.

In criminal proceedings, adversariality is guaranteed in two places in the Convention. First, in the context of general Article 6 para. 1, but also in Art. 6 par. 3, which deals exclusively with the criminal law guarantees of a fair trial. In the Criminal Procedure Code, the elements of

adversariality are also reflected in the preparatory proceedings, where the prosecutor dominus litis (lord of the dispute) and his role is to supervise the observance of the law.

The adversarial nature is typically manifested in particular in court proceedings, in the main proceedings and in the evidence taken thereon. This fact highlights the confrontation between the allegations of the accused and the prosecution, which is represented in court on behalf of the state by the prosecutor.

***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: The Slovak legal system does not specifically regulate the legal preparation for judges, prosecutor's offices, experts, lawyers for cases in which there is evidence from the mobile forensic system.

***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: Obtaining evidence from mobile devices is not limited in time in the relevant legal regulations governing their acquisition, such as Act no. 351/2011 Coll. on Electronic Communications and the Criminal Procedure Code. The time horizon is set by the operator, who must determine and justify a reasonable archiving period, because no regulation stipulates the archiving of personal data.

For individual mobile network operators - Orange, T-mobile, O2 - it is adjusted differently from 3 to 6 months, from their point of view there is no limitation period.

***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: The position of the **prosecutor** as a party to criminal proceedings is regulated in Section II. of the Criminal Procedure Code "Supervision and actions of the prosecutor", who supervises

compliance with the law before the commencement of criminal prosecution and in preparatory proceedings (§ 230 et seq. of the Criminal Procedure Code).

Criminal proceedings before a court take place only on the basis of a prosecution's indictment or a motion for an agreement on guilt and punishment, which is filed and represented before the court by the prosecutor.

After filing and representing an indictment or a motion for an agreement on guilt and punishment, the prosecutor is governed by law and huis/her internal belief based on consideration of all the evidence and the circumstances of the case.

After the indictment has been filed, **the court** will first examine it according to its content, and in cases of a crime with a lower sentence of at least 12 years, assess whether it needs to be heard in advance or whether it can order a main hearing. If the court does not transfer the case to another court or another body during the preliminary hearing, or does not suspend or dismiss the prosecution or return the case to the prosecutor to complete the investigation, it shall order the main hearing.

After the taking of evidence at the main hearing, the court may decide in the case to transfer the case, suspend the criminal prosecution, decide on conditional suspension of the criminal prosecution, conciliation or suspension of the criminal prosecution (§§ 280, 281, 282, 283 of the Criminal Procedure Code).

If the court does not decide in any of the above ways, it will decide the case by a judgment pursuant to Section 285 of the Criminal Procedure Code.

An **accused person (defendant)** is suspected of committing a criminal offense and may be considered an accused person and the means provided by this Act may be used against him/her only after an accusation/indictment has been filed against him/her (Section 33 of the Criminal Procedure Code).

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

The accused has his/her rights and obligations specified in the provisions of § 34 et seq. Criminal Procedure Code.

Witness - everyone is obliged to attend questioning once called by the authorities and the court to testify as a witness about what he/she knows about the crime and the perpetrator or about the circumstances important for criminal proceedings (§ 127 et seq. Of the Criminal Procedure Code).

A witness may not be heard on the circumstances which constitute a classified fact, unless he/she has been released from this obligation by the competent authorities - the so-called prohibition of witness examination. Exemption may be refused only if the security of the State would be endangered or other equally serious damage was threatened; the grounds for refusing an exemption must always be stated (129 of the Criminal Procedure Code).

The right to refuse to testify as a witness has the relatives of the accused directly, siblings, adoptive parent, adopted child, spouse and partner. If there are several accused and the witness is in that relationship only to one of them, he/she has the right to refuse to testify concerning other accused only if the statement concerning them cannot be separated from the statement concerning the accused with whom the witness is in this relationship - the right to refuse to resign (Section 130 of the Criminal Procedure Code).

Injured party/Victim - is a person whose health has been injured, property, moral or other damage caused, or their other legally protected rights or freedoms have been violated or endangered. In the cases provided for by this Act, the injured party has the right to express his or her consent to criminal prosecution, has the right to claim damages, make proposals for taking or supplementing evidence, submit evidence, inspect the files and study them, participate in the main hearing and at a public hearing held on an appeal or an agreement on the confession and acceptance of a sentence, to comment on the evidence presented, has the right to a final speech and the right to appeal to the extent defined by this Act.

The injured party has the right to be informed about the status of the criminal proceedings at any time during the criminal proceedings

proceedings. The information shall be provided by the prosecuting authority or the court seized of the case; for this purpose, the injured party shall be provided with the necessary contact details. Information on the status of the proceedings will not be provided if the purpose of the criminal proceedings could be jeopardized by the provision of such information (Section 46 et seq. Of the Criminal Procedure Code).

Proxies of the injured party - the injured party may be represented by proxies. An authorized representative of the organization may also be authorized to assist the injured party in assisting the injured party.

The representative of the person concerned or the injured party shall be entitled to make, on behalf of the person concerned or the injured party, proposals for the taking of evidence, to submit requests and appeals; he is also entitled to take part in all acts in which the person concerned or the injured party may take part. The injured party's representative has the right to make specific proposals for the purpose of concluding a settlement or agreement with the accused on compensation; he may also apply these proposals through a probation and mediation officer (Section 53 et seq. of the Criminal Procedure Code).

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: In the Criminal Procedure Code or in the Act on the Prosecutor's Office no. 153/2001 Coll. on the Prosecutor's Office, as amended, there are no explicit requirements for specific requirements or guidelines for the Prosecutor's Office on how to control and process mobile forensic means and evidence. Due to its position as a law enforcement body supervising the observance of legality before the commencement of criminal proceedings and in preparatory proceedings, the prosecutor ensures legality in the provision of mobile forensic means as evidence in criminal proceedings.

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: The approach and methods used to obtain, collect and analyze evidence are regulated in the relevant provisions of the Criminal Procedure Code on evidence and its execution. The area of the procedure for obtaining, collecting and analyzing evidence of telecommunications traffic records is specifically regulated in the relevant provisions of the Eavesdropping Protection Act and in the Criminal Procedure Code.

***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: This area was elaborated above in the answer to questions in Section 4. In Slovakia in criminal law in general it is well established and given that everything that can contribute to the proper clarification of the matter and what was obtained from the means of evidence under this Act may serve as evidence, or according to a special law. Evidence from a mobile phone has the same informative value as other secured evidence. In other words, evidence from a mobile phone has no advantage or higher value of evidence than other evidence.

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: The process of obtaining mobile forensic evidence is not public, it is carried out by technical departments of the police force in cooperation with mobile operators. The accused (defendant) and his/her lawyer usually meet with results only after the end of the given process in

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

the form of a transcript or in electronic form. The guarantee of legality and applicability is ensured by the legal procedure of the judge and the prosecutor, who use the relevant legal provisions for this without any doubt.

Neither the accused nor his/her lawyer have legal control over how the technical tools work and what procedures are used to obtain a record of telecommunications traffic.

The case law in the given area in the Slovak legal system is not registered.

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: Witness protection is regulated by Act no. 256/1998 Coll. on the protection of witnesses, which regulates the conditions and procedure for providing protection and assistance to endangered witnesses, protected witnesses and their relatives. The right to witness privacy is not regulated by a special regulation; it is currently difficult to exclude the publication of non-case information in the media. There are no specific requirements for witnesses regarding the ability to testify in connection with mobile forensic activities in pre-trial proceedings or in court.

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: The status and rights of the injured party/victim are mentioned in previous answers. Their protection is given in the same way as for witnesses, because the injured party usually also has the status of a witness in criminal proceedings.

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

If there is a well-founded concern that a witness or a person close to him or her is at risk of indicating the witness's place of residence, the witness may be allowed to indicate instead of residence the place of work or other address to which the call may be delivered. If a representative of a child welfare authority and a social guardianship is heard as a witness on facts which he or she has learned in connection with the implementation of child welfare and social guardianship measures, the law enforcement authority and the court shall enter in the minutes the registered office of the child welfare authority and social guardianship. (§ 136 person 1 of the Criminal Procedure Code).

If there is a reasonable concern that the witness's identity, residence or whereabouts may endanger his / her life, health, physical integrity or if such a danger is imminent to a person close to him/her, the witness may be allowed not to provide personal information. However, at the main hearing, he/she must state how he/she became acquainted with the facts which he/she had stated. Materials enabling such a witness to be identified shall be deposited with the Prosecutor's Office and in court proceedings before the President of the Chamber. They are recorded in the file only if the threat disappears. Such a witness may also, if necessary, be asked questions about the circumstances concerning his/her credibility, as well as questions concerning his/her relationship with the accused or the injured party (Section 136 (2) of the Criminal Procedure Code).

Before questioning a witness whose identity is to be kept secret, the law enforcement authority and the court shall, in the interest of protecting the witness, take measures, such as changing the witness's appearance and voice, as appropriate, or question him using technical equipment, including videoconferencing equipment (§ 136 para. 3 of the Criminal Procedure Code).

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

The applicability of a record from the mobile forensic system in the exercise of the rights of a witness - injured party is guaranteed by the principles of taking evidence and if the witness - injured party decides to use it, to point to this evidence to exercise his rights or testify, he will be legally allowed to do so.

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: It is clear from the above that the legislation in the Slovak Republic does not have established specific procedural provisions for the execution of evidence of a recording of telecommunications traffic and its special protection.

According to Slovak legislation, a record of a telecommunication operation is evidence like any other, it is equivalent and it does not take precedence over other evidence. As evidence, it is evaluated within the free evaluation of evidence together with other evidence obtained in criminal proceedings.