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:**

Law Firm Sorainen. Andris Tauriņš, Partner. Krista Niklase, Legal Assistant.

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

**Answer:**

Riga, Latvia.

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, we do not have a legally defined term for a "mobile device". Neither the Criminal Procedure Law[1] nor other laws define a term for a "mobile device". Criminal Procedure Law only states that electronic evidence is information regarding facts in the form of electronic information that has been processed, stored, or broadcast with automated data processing devices or systems.[2] Although, Operational Activities Law[3] states that the acquisition of information content from technical means can be made by telephone, by electronic or other means of communication.[4] The regulation does not specify the types of mobile devices. It is technology-neutral. However, legal doctrine explains some terms mentioned in Criminal Procedure Law:

[1] Criminal Procedure Law, *Latvijas Vēstnesis*, 74, 11.05.2005. Available at: https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law [accessed 4 August 2020].
[2] Section 136 of the Criminal Procedure Law.
[3] Operational Activities Law, *Latvijas Vēstnesis*, 131, 30.12.1993. Available at: https://likumi.lv/ta/en/en/id/57573-operational-activities-law [accessed 4 August 2020].
[4] Section 7(4) of the Operational Activities Law.

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

- automated data processing system – electronic information system, a set of computer systems, electronic networks, technical and information resources with user access;
- automated data processing devices – any device whose primary task is to perform automated data processing (computer, mobile phone, server, scanner, etc.); any such device or group of devices are considered as part of an automated data processing system.

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?*

A mobile device can be read or searched without seizing it in the inspection. This investigative action can be done if the possibility exists that **the object (mobile device) is related to the criminal offence being investigated**.[5]

The search of an automated data processing system and the data accumulated therein can be performed, if there are grounds to believe that **the information located in the specific system may contain information regarding facts included in circumstances to be proven**.[6]

A mobile device can be read or searched without seizing it also under these circumstances:

1) if the body performing operational activities has well-founded information at its disposal regarding a criminal offence prepared or having been committed by a person[7];
2) if the body performing operational activities has well-founded information at its disposal regarding a threat to national or public security caused thereby[8];

[5] Section 159(1) of the Criminal Procedure Law.
[6] Section 219(1) of the Criminal Procedure Law.
[7] Section 17(1) of the Operational Activities Law.
[8] Ibid.

3) if a person suspected, accused or convicted of committing a crime is sought[9];
4) if a person provides any assistance for the body performing operational activities in planning, committing a crime or hiding traces of a crime or help to hide a person suspected, accused of committing a crime or a convicted person who is being sought, if there are grounds for considering that the relevant operational activities measure will allow to find out the circumstances of the crime or persons committing it, to find out the location of the person to be sought, to prevent or discover threat to national or public security, or allow to identify or find out the property acquired through crime[10].

**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 some limits to this search. An official who conducts the criminal proceedings has an obligation to protect the confidentiality of the private life of a person and the commercial confidentiality of a person. Information on such confidentiality can be obtained and used only in the case where such information is necessary in order to clarify conditions that are to be proven.[11] It is also prohibited to disclose information regarding the private life of a person who participates in an investigative action, as is the disclosure of information that contains a professional secret or commercial secret, except cases where such information is necessary for proving.[12]

If information that has the significance of evidence in criminal proceedings affects a private secret of a person or affects other restricted-access information protected by law, then the person directing the proceedings restricts the spread of this information.[13]

[9] Ibid.
[10] Section 17(2) of the Operational Activities Law.
[11] Section 12(4) of the Criminal Procedure Law.
[12] Section 139(4) of the Criminal Procedure Law.
[13] Section 233(2) of the Criminal Procedure Law.

Moreover, if the information requested from such person is confidential and concerns private life protected by the law, a person has the right to immunity from criminal proceedings.[14] It means that a person has the rights to completely or partially not fulfil a criminal procedural duty, or that restricts the rights to perform specific investigative actions.[15]

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

Yes. Experts with technical knowledge have special equipment that can crack access passwords, but it is a very time-consuming process and there is no guarantee that it will really work.

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

Information can be copied at this stage. If the body performing operational activities has well-founded information at its disposal regarding a criminal offence prepared or having been committed by a person, or threat to national or public security caused thereby, or if a person suspected, accused or convicted of committing a crime is sought, can be permitted investigatory acquisition of the content of information expressed or stored by a person from technical means. That is, **downloading of the content of information or copying thereof from electronic and other types of information storage devices and information channels** owned by or at the disposal of such person.[16]

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

No, the consent of the owner/person in possession of the mobile device is not necessary. Investigatory acquisition of information stored by a person from technical means is a special investigative action. It can be performed if, in order to ascertain conditions to be proven in criminal proceedings, the acquisition of information regarding facts is necessary **without informing the person involved in the criminal proceedings and the persons who could provide such**

[14] Section 116(3) point 4 of the Criminal Procedure Law.
[15] Section 116(1) of the Criminal Procedure Law.
[16] Section 17(1) point 2 of the Operational Activities Law.

**information**.[17] The consent of the owner, possessor or holder of electronic and other types of information storage devices and information channels is not necessary for downloading the content of information or copying thereof from electronic devices.[18]

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

No. The Criminal Procedure Law does not state that unlocking the device would be obligatory in relation to such activities. It can be asked to unlock the mobile device, but the person can refuse to do so. The owner/person in possession of the mobile device cannot be forced to unlock the mobile device.

In most cases, when a person wants to cooperate, the person either removes it or gives them a password. However, there are times when police officers have to use ingenuity to get the mobile device unlocked.

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

The owner/person in possession of the mobile device must be informed in some cases. The Criminal Procedure Law provides special investigative action "control of data located in an automated data processing system". If there are grounds to believe that the information located in the specific system may contain information regarding facts included in circumstances to be proven, the search of an automated data processing system (a part thereof), the data accumulated therein, the data environment, and the access thereto, as well as the removal thereof **without the information of the owner, possessor, or maintainer of such system or data** should be performed.[19] The law provides for the possibility to search the automated data processing system

[17] Section 210(1) of the Criminal Procedure Law.
[18] Section 17(1) point 2 of the Operational Activities Law.
[19] Section 219(1) of the Criminal Procedure Law.

and data environment. The purpose of this activity is to obtain the information contained in the system without informing the owners, possessors or holders.[20]

The owner/person in possession of the mobile device **does not need to be informed before or during the action but must be informed after completion of the action**. Upon completion of an operational activities proceeding, the body performing operational activities **inform the person regarding a special method operational activities measure and time of performance thereof against whom the measure has been performed**.[21]

However, the person **should not be informed regarding operational activities performed even after completion of the action, if it may**:

1) cause damage to the lawful rights and interests of another person;
2) discover the identity of a covert assistant of operational activities or of that person or covert co-operation fact who confidentially provided assistance to the official of the body performing operational activities;
3) discover front organisations and other means of masking established for ensuring of operational activities;
4) discover organisation, methodology and tactics of operational activities measures;
5) harm the interests of national security;
6) harm the performance of the tasks of operational activities;
7) harm criminal proceedings.[22]

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

The search can be conducted with the **decision of the investigating judge or court**. The investigating judge takes the decision **based on a proposal of the person directing the**

[20] Commentary on Section 219 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 618.
[21] Section 24[1](1) of the Operational Activities Law.
[22] Section 24.[1](2) of the Operational Activities Law.

**proceedings**.[23] Although, in emergency cases where, due to a delay or objects may be destroyed, hidden, or damaged, a search can be performed with a **decision of the person directing the proceedings**. If a decision is taken by an investigator then a search can be performed with **the consent of a prosecutor**.[24]

Formal requirements of the search:

1) The decision on a search should indicate who will search and remove, where, with whom, in what case, and the objects that will be sought and withdrawn[25];
2) The decision on a search should not be necessary in conducting a search of a person to be detained[26];
3) The search should be conducted in the presence of the person at whose site the search takes place, or in the presence of a family member of legal age of such person[27];
4) A search should be conducted in the presence of a suspect or accused person if it takes place in the declared place of residence and work place of the referred to persons, except the case where it is not possible due to objective reasons[28];
5) In order to identify the objects being sought, a victim or witness may also be invited to a search[29];
6) The rights of persons located at the site of a search to be present during the entire term of the operations of the performer of the investigative action, and to express the remarks thereof regarding such operations, should be explained to such persons[30];
7) A performer of an investigative action, together with the persons present during the investigative action, is entitled to enter into the premises or geographical territory indicated

[23] Section 180(1) of the Criminal Procedure Law.
[24] Section 180(3) of the Criminal Procedure Law.
[25] Section 180(2) of the Criminal Procedure Law.
[26] Section 180(4) of the Criminal Procedure Law.
[27] Section 181(1) of the Criminal Procedure Law.
[28] Section 181(3) of the Criminal Procedure Law.
[29] Section 181(4) of the Criminal Procedure Law.
[30] Section 181(5) of the Criminal Procedure Law.

in a decision on a search in order to find the objects being sought mentioned in the decision[31].

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

No, in general, it does not matter whether this person is the accused or witness/third party or the victim. Although, in some cases it could matter. For example:

1) The search should be conducted in the presence of a suspect or accused person if it takes place in the declared place of residence and work place of the referred to persons, except the case where it is not possible due to objective reasons[32];
2) In order to identify the objects being sought, a victim or witness may also be invited to a search[33];
3) If a victim or witness present at a search recognises one of the found objects, such finding should be indicated in the minutes of search[34].

***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.*

The Latvian legislation does not prescribe any specific procedure to access data stored in the Cloud. Data stored in the cloud can be accessed on the same conditions as other data on the mobile device.

Therefore, regarding the information stored in the cloud, the police in Latvia have had little contact with it. As with any information containing data, the judge's consent is required to allow such information to be requested, and then from who holds this information the European Investigation Order or request for legal assistance is sent.

[31] Section 182(1) of the Criminal Procedure Law.
[32] Section 181(3) of the Criminal Procedure Law.
[33] Section 181(4) of the Criminal Procedure Law.
[34] Section 182(7) of the Criminal Procedure Law.

If it is necessary to carry out the control of means of communications in the territory of one or several European Union Member States, but technical assistance of the relevant European Union Member States is not necessary, the person directing the proceedings completes a notification of a special form by informing on carrying out the control of means of communication in the territory of the European Union Member State and send it to such Member State.[35] Then, if the information is received from a European Union Member State that the control of means of communication would not be permissible for the same offence in this Member State, the person directing the proceedings does not commence or terminate the control of means of communication.[36]

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

Yes. In cases where immediate action is required to avert or detect terrorism, murder, gangsterism, riots, other serious or especially serious crime, as well as where the lives, health or property of persons are in real danger, the operational activity measures (investigatory acquisition of information expressed or stored by a person by technical means) can be performed with the approval of a prosecutor. In that case, approval of a judge must be obtained on the following working day, but not later than within 72 hours.[37]

***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. Information regarding facts that has been obtained by allowing other procedural violations can be considered restrictedly admissible, and may be used in proving only in the case where:

- the allowed procedural violations are not essential or may be prevented;
- or such violations have not influenced the veracity of the acquired information;

[35] Section 887[4](1) of the Criminal Procedure Law.
[36] Section 887[4](2) of the Criminal Procedure Law.
[37] Section 7(5) of the Operational Activities Law.

- or if the reliability of such information is approved by the other information acquired in the proceedings.[38]

Obtaining factual information in violation of the principles of criminal procedure (for example, guaranteeing human rights) makes this information inadmissible and unusable as evidence.[39] In addition, evidence acquired in a conflict of interest situation can be allowed only if a maintainer of prosecution is able to prove that the conflict of interests has not influenced the objective progress of the criminal proceedings.[40]

*Mobile device seized*

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

Yes, the mobile device (e.g. a smartphone) can be seized. Although no regulation directly states this, it can be deduced from the definition of withdrawal (seizing). In this investigative action can be removed objects significant in a case.[41]

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

The withdrawal should be conducted with **the decision of the person directing the proceedings**.[42] The decision on withdrawal indicates who will perform withdrawal of an object, where, with whom, in what case, and the objects that will be withdrawn.[43]

The formal requirements or withdrawal:

1) Upon commencing a withdrawal, the performer of the investigative action should present the decision to the person at whose site the withdrawal is being conducted. The person

[38] Section 130(3) of the Criminal Procedure Law.
[39] Commentary on Section 12 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 60.
[40] Section 130(4) of the Criminal Procedure Law.
[41] Section 186 of the Criminal Procedure Law.
[42] Section 187(1) of the Criminal Procedure Law.
[43] Section 187(2) of the Criminal Procedure Law.

should sign therefor in the decision. Then the performer of the investigative action should invite the person to issue the object being withdrawn without delay.[44]

2) Withdrawn objects should be described in the minutes of the withdrawal.[45]
3) After completion of the investigative action, a copy of the minutes of a withdrawal and of the decision should be issued to the person at whose site the withdrawal was conducted.[46]
4) If a person refuses to issue an object to be withdrawn, or if the object cannot be found in the indicated location and there are grounds to believe that such object is located elsewhere, the decision to conduct a search may be taken, and the search may be conducted in order to find such object.[47]

However, there is also an option to seize the mobile device without conducting the withdrawal. In this situation, the person directing the proceedings is entitled to request from natural or legal person objects, including in the form of electronic information and document that is processed, stored or transmitted using electronic information systems.[48] This action is intended for:

- data that does not need to be stored immediately;
- data that does not contain personal correspondence;
- data that is not stored an electronic information system of the merchant of this system (data to be retained).[49]

But if natural or legal persons do not submit the objects requested by the person directing the proceedings, the person directing the proceedings can conduct a withdrawal or search.[50]

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

[44] Section 188(1) of the Criminal Procedure Law.
[45] Section 188(2) of the Criminal Procedure Law.
[46] Section 188(3) of the Criminal Procedure Law.
[47] Section 188(4) of the Criminal Procedure Law.
[48] Section 190(1) of the Criminal Procedure Law.
[49] The Information Technology Security Incident Response Institution of the Republic of Latvia. Pierādījumu saglabāšanas principi IT vidē notikušos noziegumos. Available: https://cert.lv/uploads/pasakumi/Aleksandrs_Buko_elektroniskie_pieradijumi_updated.pdf [accessed 4 August 2020].
[50] Section 190(2) of the Criminal Procedure Law.

Yes, information can be copied. If the body performing operational activities has well-founded information at its disposal regarding a criminal offence prepared or having been committed by a person, or threat to national or public security caused thereby, or if a person suspected, accused or convicted of committing a crime is sought, can be permitted investigatory acquisition of the content of information expressed or stored by a person from technical means. That is, downloading of the content of information or copying thereof from electronic and other types of information storage devices and information channels owned by or at the disposal of such person.[51]

***19.*** *Are there any limits to this search (e.g. core area of private life, privacy limits, limits defined by the crime, limits defined by the order/warrant)? If so, how precise are these/must these be defined?*

Please look at the answer to question 5.

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

No. Investigatory acquisition of information stored by a person from technical means is a special investigative action. It can be performed if, in order to ascertain conditions to be proven in criminal proceedings, the acquisition of information regarding facts is necessary **without informing the person involved in the criminal proceedings and the persons who could provide such information**.[52] The consent of the owner, possessor or holder of electronic and other types of information storage devices and information channels is not necessary for downloading the content of information or copying thereof from electronic devices.[53]

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

No. The Criminal Procedure Law does not state that unlocking the device would be obligatory in relation to such activities. It can be asked to unlock the mobile device, but the person can refuse to

[51] Section 17(1) point 2 of the Operational Activities Law.
[52] Section 210(1) of the Criminal Procedure Law.
[53] Section 17(1) point 2 of the Operational Activities Law.

do so. The owner/person in possession of the mobile device cannot be forced to unlock the mobile device.

In most cases, when a person wants to cooperate, the person either removes it or gives them a password. However, there are times when police officers have to use ingenuity to get the mobile device unlocked.

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

The owner/person in possession of the mobile device must be informed in some cases. Criminal Procedure Law provides investigative action "disclosure and issue of data stored in an electronic information system". In this case during the pre-trial criminal proceedings, an investigator with the consent of a prosecutor or a data subject and a prosecutor with the consent of a higher-ranking prosecutor or a data subject **may request**, that the merchant of an electronic information system disclose and issue the data to be stored in the information system.[54]

The legislator has provided that traffic data may be disclosed if the data subject has given specific consent. A data subject is a natural person who can be directly or indirectly identified by stored traffic data. Thus, if the person directing the proceedings obtains the consent of such a data subject to process this data, then he/she may request and disclose the traffic data without the consent of the prosecutor. If the consent of the traffic data subject for the disclosure of data has not been received, then the person directing the proceedings is obliged to apply to the prosecutor and the data should be issued and disclosed only with the consent of the prosecutor. Thus, the owner/person in possession of the mobile device is informed if the person directing the proceedings initially contacts the data subject for getting consent.[55]

[54] Section 192(1) of the Criminal Procedure Law.
[55] Commentary on Section 192 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 573.

Criminal Procedure Law also provides special investigative action "control of data located in an automated data processing system". If there are grounds to believe that the information located in the specific system may contain information regarding facts included in circumstances to be proven, the search of an automated data processing system (a part thereof), the data accumulated therein, the data environment, and the access thereto, as well as the removal thereof without the information of the owner, possessor, or maintainer of such system or data, should be performed.[56]

The law provides not only for the possibility to search the automated data processing system and data environment but also for the removal of information that may contain information about the facts included in the circumstances to be proved.[57] It is similar to the withdrawal of objects and documents during a search.[58] The purpose of this activity is to obtain the information contained in the system without the awareness of the owners, possessors or holders.[59]

Therefore, the owner must be informed, depending on the investigative action taken.

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

Yes. Experts with technical knowledge have special equipment that can crack access passwords, but it is a very time-consuming process and there is no guarantee that it will really work.

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

Please look at the answer to question 12.

***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*

[56] Section 219(1) of the Criminal Procedure Law.
[57] Commentary on Section 219 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 618.
[58] Section 182(6) of the Criminal Procedure Law.
[59] Commentary on Section 219 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 618.

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

Please look at the answer to question 13.

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

Please look at the answer to question 13.

***27.*** *Can you legally access data in the Cloud, even if there is no app that links to this data or other direct link from the mobile device?*

Please look at the answer to question 13.

***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?*

Criminal Procedure Law provides investigative action "disclosure and issue of data stored in an electronic information system". In this case during the pre-trial criminal proceedings may be requested that the merchant of an electronic information system discloses and issue the data to be stored in the information system.[60] Depending on the stage of criminal procedure, there are two options on how it can be requested, that the merchant of an electronic information system disclose and issue the data to be stored in the information system:

1) during the pre-trial criminal proceedings an **investigator with the consent of a prosecutor or a data subject and a prosecutor with the consent of a higher-ranking prosecutor or a data subject**[61];
2) in trying a criminal case, **a judge or the court panel**[62].

[60] Section 192(1) of the Criminal Procedure Law.
[61] Section 192(1) of the Criminal Procedure Law.
[62] Section 192(3) of the Criminal Procedure Law.

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

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

Please look at the answer to question 14.

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

Please look at the answer to question 15.

*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.

***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:**

An inspection of the automated data processing system (a part thereof) should not be usually performed on site, but such system (a part thereof) should be withdrawn, ensuring retaining of data completeness in an unmodified condition.[63] It follows that the principle of data integrity requires that the removal must ensure that the integrity of the data remains unchanged. Of the basic principles of police electronic evidence validation, no action by a procedurally authorised person should result in a change to data stored on a computer or other media (for example, changes to files when a computer is turned on).[64]

However, obtaining electronic information in order to comply with the principles of obtaining electronic evidence requires special technical knowledge. The person must be able to explain the changes. Therefore, in criminal proceedings, inspections are often performed with the participation of a specialist. In this case, everything that is done must be recorded. When handling electronic evidence, it is important to provide audio transcripts or other descriptions that will explain in detail all the processes that were used for the evidence. There is no publically available information on what rules the protocol is based and what are specific requirements.

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

**Answer:**

No, we do not have any specific rules in criminal procedure that regulate the use of mobile forensics tools using/deploying AI technology. Neither the Criminal Procedure Law nor other laws regulate the use of mobile forensics tools using AI technology. General rules apply to AI technology.

[63] Section 160(6) of the Criminal Procedure Law.
[64] The Information Technology Security Incident Response Institution of the Republic of Latvia. Pierādījumu saglabāšanas principi IT vidē notikušos noziegumos. Available: https://cert.lv/uploads/pasakumi/Aleksandrs_Buko_elektroniskie_pieradijumi_updated.pdf [accessed 4 August 2020].

***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:**

In order to perform search and access to automated data processing systems, data stored in it and search of data environment, as well as withdrawal outside Latvia, the person directing the proceedings must act in accordance with the provisions of the Criminal Procedure Law regarding the request to a foreign country regarding the performance of procedural actions (Chapter 83).[65]

It should be noted that if a specialised public authority has authorised (i.e. access with a single access identifier and password) access to automated data processing systems of the same authority, company or person through interception points, and if they are geographically located in different locations, then a new decision of the investigating judge is not required. This condition also applies to such foreign companies registered and conducting business in Latvia, whose automated data processing systems form a unified data transmission network both in the territory of Latvia and abroad.[66]

If the performance of a procedural action in a foreign country is necessary in criminal proceedings, the person directing the proceedings turns to the competent authority with a written proposal to request that the foreign country performs the procedural action.[67]

Execution of a procedural action requested in a European Investigation Order should take place by complying with the procedures laid down in Criminal Procedure Law regarding the performance

[65] Commentary on Section 219 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 619.
[66] Commentary on Section 219 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 620.
[67] Section 876(1) of the Criminal Procedure Law.

of procedural actions and international co-operation in the field of criminal law.[68] Consequently, national law and the procedural regulation provided for therein are applicable to the performance of procedural actions.

***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:**

The Criminal Procedure Law prescribes the procedure for submitting a request to a foreign country regarding the performance of procedural actions (Chapter 83), as well as specific provisions directly related to the European Investigation Order (Chapter 82.[1] and Chapter 83.[1]). There is no established procedure/course of action to decide whether to apply the EIO or another instrument for cross-border gathering of evidence within the EU. The Criminal Procedure Law must be followed, which states that in order to obtain new or existing evidence from the territory of another Member State of the European Union, it is necessary to fill in a special form document – the European Investigation Order.[69]

***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:**

Latvia requests international co-operation in criminal matters from a foreign country, and ensures such co-operation:

1) in the extradition of a person for a criminal prosecution, trial, or the execution of a judgment, or for the determination of compulsory measures of a medical nature;
2) in the transfer of criminal proceedings;
3) in the execution of procedural actions;

[68] Section 875.[8] of the Criminal Procedure Law.
[69] Section 875.[1] of the Criminal Procedure Law.

4) in the execution of a security measure not related to deprivation of liberty;
5) in the recognition and execution of a judgment;
6) in other cases provided for in international treaties.[70]

Latvia has concluded several mutual legal assistance treaties in criminal matters, for example, with the Russian Federation[71], the United States[72], Ukraine[73], Belarus[74], Uzbekistan[75], Poland[76], China[77], Kyrgyzstan[78] and Moldova[79]. Also, this year in February, the representatives of Latvia agreed to continue negotiations on a legal assistance agreement in criminal matters with the Republic of South Africa.[80]

[70] Section 673(1) of the Criminal Procedure Law.
[71] Agreement between the Republic of Latvia and the Russian Federation on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters. Available at: https://likumi.lv/ta/lv/starptautiskie-ligumi/id/533-ligums-starp-latvijas-republiku-un-krievijas-federaciju-par-tiesisko-palidzibu-un-tiesiskajam-attiecibam-civilajas-gimenes
[72] Law on the Agreement on Mutual Legal Assistance between the European Union and the United States of America,. Available at: https://likumi.lv/ta/id/121223-par-eiropas-savienibas-un-amerikas-savienoto-valstu-savstarpejas-tiesiskas-palidzibas-ligumu
[73] Law On the Agreement between the Republic of Latvia and Ukraine on Legal Assistance and Legal Relations in Civil, Family, Labor and Criminal Matters. Available at: https://likumi.lv/ta/id/52763-par-latvijas-republikas-un-ukrainas-ligumu-par-tiesisko-palidzibu-un-tiesiskajam-attiecibam-civilajas-gimenes-darba-un-kriminallietas
[74] Law on the Agreement between the Republic of Latvia and the Republic of Belarus on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters. Available at: https://likumi.lv/ta/id/33834-par-ligumu-starp-latvijas-republiku-un-baltkrievijas-republiku-par-tiesisko-palidzibu-un-tiesiskajam-attiecibam-civilajas-gimenes
[75] Law on the Agreement between the Republic of Latvia and the Republic of Uzbekistan on Legal Assistance and Legal Relations in Civil, Family, Labor and Criminal Matters. Available at: https://likumi.lv/doc.php?id=40614
[76] Law on the Agreement between the Republic of Latvia and the Republic of Poland on Legal Assistance and Legal Relations in Civil, Family, Labor and Criminal Matters. Available at: https://likumi.lv/doc.php?id=33833
[77] Law on the Agreement between the Republic of Latvia and the People 's Republic of China on Mutual Legal Assistance in Criminal Matters. Available at: https://likumi.lv/ta/id/94547-par-latvijas-republikas-un-kinas-tautas-republikas-ligumu-par-savstarpejo-tiesisko-palidzibu-kriminallietas
[78] Law on the Agreement between the Republic of Latvia and the Kyrgyz Republic on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters. Available at: https://likumi.lv/ta/id/48411-par-latvijas-republikas-un-kirgizijas-republikas-ligumu-par-tiesisko-palidzibu-un-tiesiskajam-attiecibam-civilajas-gimenes-un-kriminallietas
[79] Law on the Agreement between the Republic of Latvia and the Republic of Moldova on Legal Assistance and Legal Relations in Civil, Family and Criminal Matters. Available at: https://likumi.lv/ta/id/37059-par-latvijas-republikas-un-moldovas-republikas-ligumu-par-tiesisko-palidzibu-un-tiesiskajam-attiecibam-civilajas-gimenes-un-kriminallietas
[80] Ministry of Foreign Affairs of the Republic of Latvia. Latvian officials in the RSA agree on continuing negotiations on a legal assistance agreement in criminal matters. Available: https://www.mfa.gov.lv/en/news/latest-news/65597-latvian-officials-in-the-ras-agree-on-continuing-negotiations-on-a-legal-assistance-agreement-in-criminal-matters [accessed 4 August 2020].

Coordinating and promoting mutual criminal co-operation, the Eurojust has powers to request the competent authorities of the Member States to investigate the specific criminal offences and institute the cases, to recognise that one Member State is in a better position for investigation or prosecution of a specific criminal offence than another, to coordinate the work of the competent authorities, to set up the joint investigation team, as well as to request an information needed for fulfilment of the Eurojust tasks. During the period from 1 January to 30 June 2020, Latvian representation in Eurojust has opened 30 new cases based on a request for assistance from the competent Latvian authorities. During the reporting period, Eurojust's capacity to promote and coordinate international criminal co-operation was mostly used by the State Police and the Prosecutor's Office, but less by the courts.[81]

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

**Answer:**

The person directing the proceedings, without conducting the withdrawal, is entitled to request from any natural or legal persons, in writing, objects, documents and information regarding the facts that are significant to criminal proceedings, including in the form of electronic information and document that is processed, stored or transmitted using electronic information systems.[82] In practice, such requests are sent to the private sector on a very regular basis as part of criminal proceedings.

If natural or legal persons do not submit the objects and documents requested by the person directing the proceedings during the term specified by such person directing the proceedings, the

[81] The Prosecution Office. Overview of the work of the Representation of the Republic of Latvia at Eurojust from 1 January to 30 June 2020. Available: http://www.prokuratura.gov.lv/media/Parskats_par_darbibu_01.01.2020-30.06.2020.docx [accessed 4 August 2020].
[82] Section 190(1) of the Criminal Procedure Law.

person directing the proceedings should conduct a withdrawal or search in accordance with the procedures laid down in Criminal Procedure Law.

On the other hand, in some cases, legal persons may be required not only for data already in their possession but also to create new data, for example, an audit, inventory, resoric or service inspection may be required.[83] The heads of legal persons have a duty to perform a documentary audit, inventory, or departmental or service examination within the framework of the competence thereof and upon a request of the person directing the proceedings, and to submit documents, within a specific term, together with the relevant additions regarding the fulfilled request.[84]

[83] Commentary on Section 190 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 568.
[84] Section 190(3) of the Criminal Procedure Law.

## 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:**

- *Data protection concerns (Law Enforcement Directive 2016/680 and implementing national law)*

In August 2019, a new law "On the processing of personal data in criminal proceedings and administrative violation proceedings"[85] entered into force. Its purpose is to protect the fundamental rights of natural persons, in particular the right to privacy, when the competent authorities process personal data in order to investigate criminal offences.[86]

[85] Law on the processing of personal data in criminal proceedings and administrative violation proceedings, *Latvijas Vēstnesis*, 147, 22.07.2019. Available at: https://likumi.lv/ta/id/308278-par-fizisko-personu-datu-apstradi-kriminalprocesa-un-administrativa-parkapuma-procesa [accessed 4 August 2020].
[86] Section 2 of the Law on the processing of personal data in criminal proceedings and administrative violation proceedings.

The new law maintains the principles of personal data processing similar to the general regulation. For example, the processing of data of authorities is lawful only if and to the extent that such processing is necessary for the performance of the task performed by the competent authority for the above purposes. Data processing must not be excessive (i.e. purpose limitation). The controller must also comply with data processing principles such as accuracy, storage limitation, storage security, etc. The regulation also preserves the same rights of the data subject as provided for in the General Data Protection Regulation, and they are set out in Articles 10-14 of the 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)*

In particular, the prosecutor or the court must assess whether the public benefit from the disclosure of data stored in an electronic information system for use in requesting and disclosing it in criminal proceedings for criminal offences and less serious crimes will outweigh the violation of fundamental rights of the individual.[87]

Since, when adjudicating a case, a court or a judge ensures the rule of law in criminal proceedings, the legislator has given the court the right to request any kind of data necessary to adjudicate the case regarding the specific criminal offence. However, in making such a request, the court must carefully assess the proportionality and necessity of such a measure.[88]

The investigating judge must also very carefully assess the circumstances of the case and the proportionality of the special investigative activity (control of the content of the transmitted data) with the invasion of privacy.[89] When substantiating the need for a special investigative action, the proposal should indicate the information obtained as a result of the investigative action, which

[87] Commentary on Section 192 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 573.
[88] Ibid.
[89] Commentary on Section 220 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 622.

indicates the need to initiate or continue data control in the criminal proceedings under investigation.[90]

The person directing the proceedings should use all the measures provided for by law in order to restrict the spread of information that has been acquired as a result of a special investigative action and that has the significance of evidence in criminal proceedings if such information affects a private secret of a person or affects other restricted-access information protected by law.[91]

An official who conducts the criminal proceedings has the obligation to protect the confidentiality of the private life of a person and the commercial confidentiality of a person. Information on such confidentiality can be obtained and used only in the case where such information is necessary in order to clarify conditions that are to be proven.[92] Information obtained in the course of a special investigation action which concerns the privacy of individuals must be carefully assessed by the person directing the proceedings, and information which does not relate to verifiable circumstances, including privacy, should not be included in the transcripts, sound recordings and video recordings.[93]

It is also prohibited to disclose information regarding the private life of a person who participates in an investigative action, as is the disclosure of information that contains a professional secret or commercial secret, except cases where such information is necessary for proving.[94]

It is the duty of the person directing the proceedings to react to violations of certain restrictions of the persons warned in the proceedings and, if such are established, to resolve the issue of liability

[90] Commentary on Section 220 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 622.
[91] Section 233(2) of the Criminal Procedure Law.
[92] Section 12(4) of the Criminal Procedure Law.
[93] Commentary on Section 221 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 623.
[94] Section 139(4) of the Criminal Procedure Law.

of persons for disclosure of information obtained in pre-trial criminal proceedings or criminal liability of officials.[95]

- *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)*

The Criminal Procedure Law should determine a uniform procedural order for all persons involved in criminal proceedings irrespective of the origin, social and financial situation, employment, citizenship, race, nationality, attitude toward religion, sex, education, language, place of residence, and other conditions of such persons.[96] If the difference in attitude is based on a prohibited criterion, it is not permissible and it is no longer necessary to examine whether that difference has reasonable grounds, has legitimate aims and is proportionate.[97]

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

The obligation to store data is regulated in the Criminal Procedure Law – the duty to store data located in an electronic information system may be specified for a term of up to 30 days, but such term may be extended, if necessary, by an investigating judge by a term of up to 30 days.[98] This action applies to an existing set of data stored in the system. Its task is to prevent this data from being altered, obscured or otherwise deteriorated. This can be any data, including location data, traffic data, and content data if they are stored in system memory. The purpose of this procedural step is to ensure that the data is preserved for up to 30 days in an unaltered state. Further, the retention period of preserved data can be extended up to 30 days only by a decision of the investigating judge. Thus, in a decision taken by the person directing the proceedings against a

[95] Commentary on Section 233 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 654.
[96] Section 8 of the Criminal Procedure Law.
[97] Commentary on Section 8 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 49.
[98] Section 191(2) of the Criminal Procedure Law.

particular person regarding the retention of data contained in his/her system, the retention may not exceed a total of 60 days.[99] Only a small amount of specific data may be subject to this decision on the retention of data stored in the system if it is directly related to the need to prove in a specific criminal proceeding. Consequently, it means that the person directing the proceedings must use the tool to ensure proportionality between the potential harm to the person charged with the preservation of data in criminal proceedings and the harm of the specific offence. This decision cannot require the subject to disclose encrypted information. Also, the content of the decision must not violate the right of the suspect or accused not to testify against himself.[100]

In turn, another term for data retention is specified in the Electronic Communications Law[101]. The data retention set forth herein refers to data that is currently generated and will be in the possession of someone in the future.[102] These data include load and location data, which the trader is obliged to keep for 18 months.[103]

When authorising the removal or copying of data, the investigating judge must assess their applicability to the offence under investigation or other crime, as well as unjustified invasion of privacy, professional or trade secrets, withdrawing or copying data. Without an initial search of the automated data processing system, it may not be clear about the details of the evidence to be demonstrated in the system. Therefore, in the initiation, the person directing the proceedings needs to indicate as much as possible from the outset exactly what factual information has been clarified and what data must be removed from the case file, for example, information received from partner

[99] Commentary on Section 191 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 570.
[100] Commentary on Section 191 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 571.
[101] Electronic Communications Law, *Latvijas Vēstnesis*, 183, 17.11.2004. Available at: https://likumi.lv/ta/en/en/id/96611-electronic-communications-law [accessed 4 August 2020].
[102] Commentary on Section 191 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 570.
[103] Section 71.[1](8) and 19(1) point 11 of the Electronic Communications Law.

services indicates the involvement of the subject in the distribution of child pornography or the subject's electronic correspondence with the joint participants of offence. The proposal should specify which data already known should otherwise be retained, for example by instructing the data holder, who is not a joint participant in a criminal offence, to retain them, what copies of the data need to be made and by whom.[104]

[104] Commentary on Section 219 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 620.

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:**

There are no rules or guidelines on the admissibility of electronic evidence in our jurisdiction applicable to mobile forensics. However, there are general rules which also apply to electronic evidence.

It should be admissible to use information regarding facts acquired during criminal proceedings, if such information was obtained and procedurally fixed in accordance with the procedures laid down in Criminal Procedure Law.[105] Information regarding facts that has been acquired in the following manner should be recognised as inadmissible and unusable in proving:

- using violence, threats, blackmail, fraud, or coercion;
- in a procedural action that was performed by a person who, in accordance with the Criminal Procedure Law, did not have the right to perform such operation;
- allowing the violations specially indicated in the Criminal Procedure Law that prohibits the use of a specific piece of evidence;
- violating the fundamental principles of criminal proceedings.[106]

Information regarding facts that has been obtained by allowing other procedural violations should be considered restrictedly admissible, and may be used in proving only in the case where the allowed procedural violations are not essential or may be prevented, or such violations have not influenced the veracity of the acquired information, or if the reliability of such information is approved by the other information acquired in the proceedings.[107]

[105] Section 130(1) of the Criminal Procedure Law.
[106] Section 130(2) of the Criminal Procedure Law.
[107] Section 130(3) of the Criminal Procedure Law.

Information used in evidence in criminal proceedings may be obtained and provisionally confirmed only in accordance with the procedures specified by the Criminal Procedure Law. However, in certain cases, information obtained outside the criminal proceedings is also allowed, the use of which in the criminal proceedings is permitted if certain preconditions are met. For example, it is information obtained during operational activities that can be used in evidence.[108] For example, it is not permissible to use as evidence information about facts obtained by police officers actually carrying out an operational measure without complying with the requirements of the Operational Activities Law.[109] If the information on the facts has been obtained in violation of the procedures specified in the Operational Activities Law, there is the highest probability that such information cannot be used as evidence in a particular criminal proceeding.[110]

Thus, for the use of information by not applying the Criminal Procedure Law but criminal procedure laws of other countries, in Latvia has significant requirements for assessing the admissibility of evidence and recognising evidence as inadmissible or restricted. In order to recognise that information about facts obtained as a result of criminal co-operation cannot be used in evidence, the court must establish one of the conditions of inadmissibility of evidence specified by the Criminal Procedure Law[111]:

- using violence, threats, blackmail, fraud, or coercion;
- in a procedural action that was performed by a person who, in accordance with the Criminal Procedure Law, did not have the right to perform such operation;

[108] Commentary on Section 130 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 439.
[109] Supreme Court of the Republic of Latvia 28.12.2015. decision in criminal case No. 11903022711 (SKK-549/2015). Available at: http://at.gov.lv/downloadlawfile/3692 [accessed 4 August 2020].
[110] Supreme Court of the Republic of Latvia 25.11.2014. decision in criminal case No. 11819003409 (SKK-0490-14). Available at: https://manas.tiesas.lv/eTiesasMvc/nolemumi/pdf/194689.pdf [accessed 4 August 2020].
[111] Commentary on Section 130 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 440.

- allowing the violations specially indicated in the Criminal Procedure Law that prohibit the use of a specific piece of evidence;
- violating the fundamental principles of criminal proceedings[112].

***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:**

Yes, the criteria for admissibility of evidence collected through mobile forensics are the same as for the other type of evidence, because there are no rules or guidelines on the admissibility of electronic evidence in our jurisdiction applicable to mobile forensics. The Criminal Procedure Law only regulates general rules which also apply to electronic 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:**

Two aspects need to be considered when describing the admissibility requirements: 1) information was obtained in accordance with the procedures laid down in this Criminal Procedure Law and 2) information was procedurally fixed in accordance with the procedures laid down in Criminal Procedure Law.[113] Thus, information used in evidence in criminal proceedings may be obtained and procedurally confirmed only in accordance with the procedures specified by the Criminal Procedure Law. Therefore, if procedural rules are not followed, evidence from mobile forensics cannot be submitted to the Court.

Evidence should be admissible if the information contained therein:

1) obtained from sources of factual information provided by law;

[112] Section 130(2) of the Criminal Procedure Law.
[113] Section 130(1) of the Criminal Procedure Law.

2) acquired by competent entities;
3) obtained and procedurally strengthened in the manner prescribed by law (including the use of unauthorised techniques and methods);
4) if other provisions of the law have been complied with, which have been set as a mandatory precondition for the procedural use of information as evidence.[114]

If in the course of obtaining or procedural confirmation of information the requirements of the law have not been complied with, there is reason to doubt the admissibility of the use of this information in proof. In order to determine the significance of a procedural defect in the admissibility of evidence, only the gravity and nature of the infringement are relevant. Thus, for example, the degree of harm, the nature of the criminal offence, the characteristics of the persons involved are not relevant in assessing this issue.

Depending on the nature of the infringement, its effect can be divided into two types:

1) The information should be declared inadmissible and unusable in evidence (**absolute inadmissibility**). Information regarding facts that has been acquired in the following manner should be recognised as inadmissible and unusable in proving:
    - using violence, threats, blackmail, fraud, or coercion;
    - in a procedural action that was performed by a person who, in accordance with the Criminal Procedure Law, did not have the right to perform such operation;
    - allowing the violations specially indicated in the Criminal Procedure Law that prohibits the use of a specific piece of evidence;
    - violating the fundamental principles of criminal proceedings.[115]
2) The information can be used in evidence, but only if certain preconditions are met (**limited admissibility**). The admissibility of information is limited in cases where:

[114] Commentary on Section 130 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 440.
[115] Section 130(2) of the Criminal Procedure Law.

- the violations committed in obtaining them are not so significant as to cause absolute inadmissibility;
- the procedural violations are insignificant;
- the committed procedural violations can be eliminated;
- the procedural irregularities committed could not affect the veracity of the information obtained;
- the reliability of the information is confirmed by other information obtained in the process.[116]

***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:**

If the person directing the proceedings receives a decision of an investigating judge on a search of an automated data processing system in the territory of Latvia, but accesses data in a data warehouse in another country without using additional access identifiers (passwords and usernames), then in accordance with Article 32 of the Cybercrime Convention, such access and removal without informing the country in which the data warehouse or electronic service provider is located should be permitted only with the written consent of the data subject.[117]

***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*

[116] Commentary on Section 130 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 445.
[117] Commentary on Section 219 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 620.; Ķinis U. Kibernoziedzība, kibernoziegumi un jurisdikcija. Rīga: Jumava, 2015, p. 404–406.

*(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:**

Any information retrieved from storage media (from computers, tablets, USB, hard drives, mobile phones, etc.) is copied or a clone is created in order not to damage the original information on the device. A checksum is calculated that coincides with the same data set that was copied, thus proving that both data sets, both the original and the created copy or clone, are identical, maintaining the integrity of the data. Although, any alteration may not render the evidence inadmissible. The information can be used in evidence, for example, if the alteration is not so significant as to cause absolute inadmissibility, or the alteration could not affect the veracity of the information obtained.

***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:**

No, the Criminal Procedure Law does not regulate any rules on the used technology, methodology or standard, such as for example that this must be forensically sound as a prerequisite for admissibility.

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

**Answer:**

No, unfortunately, there is no case law available in a publicly available database of court decisions regarding the admissibility of evidence produced using mobile forensics.

***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:**

No, our regulation is based only on general rules, There is no specific standardisation on digital evidence. It is only stated that the person directing the proceedings must follow the following principles for obtaining e-evidence from the European Union Agency for Cybersecurity (www.enisa.europa.eu):

1) Data integrity – data must be kept unchanged regardless of the type and stage of their acquisition;
2) Process auditing – the person directing the proceedings must document the process of ensuring the consistency of the data, from the acquisition of evidence to the moment it is recognised and attached as evidence in the case;
3) Specialist support – to solve technical problems that may arise in the process of taking e-evidence.[118]

***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 admissibility of information is limited when it can be used in evidence, but certain preconditions must be met in cases where:

- the violations committed in obtaining them are not so significant as to cause absolute inadmissibility;
- the procedural violations are insignificant;

[118] Commentary on Section 136 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 459.

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

- the committed procedural violations can be eliminated;
- the procedural irregularities committed could not affect the veracity of the information obtained
- the reliability of the information is confirmed by other information obtained in the process.

Consequently, the use of procedurally defective information requires several preconditions at the same time. That whether the failure to comply with Data Protection law, or privacy rules in itself, is enough to refuse admissibility of the evidence, even when the procedure is otherwise followed, is not directly regulated. In this case, the above preconditions should be assessed. However, such an infringement is not likely to automatically lead to the inadmissibility of the evidence. In such a situation, the evidence is likely to be admissible as admissible evidence because there has been a minor procedural irregularity in the process of obtaining it.

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

**Answer:**

No, unfortunately, in the available database of anonymised court rulings, the court decisions that mention electronic evidence are only mentioned but not analysed.

## 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:**

- *Is mobile forensic evidence given a certain probative value?*

No, there is no special value for mobile forensic evidence. They have the same value as any other evidence. In criminal proceedings, all evidence must be assessed in conjunction with other evidence, without any of them giving a higher degree of reliability.

- *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 only general rules. The reliability of the information regarding facts that is to be used in proving should be assessed by considering all the facts, or information regarding facts, acquired during criminal proceedings as a whole and in the mutual relation thereof.[119]

[119] Section 128(2) of the Criminal Procedure Law.

This means that, although reliability is an inherent feature of each individual evidence, it can only be determined by looking at the evidence in a single system with other evidence and assessing how they interact. It remains to be seen whether the reliability of the evidence in question will be corroborated by other evidence.[120]

No piece of evidence has a previously specified degree of reliability higher than other pieces of evidence.[121] This means that all the evidence must initially be considered equally reliable. None of the evidence is superior in terms of reliability.[122] For example, it follows from the case law that the Criminal Procedure Law does not restrict the detection of the effects of alcohol to the use of a portable device to determine the effects of alcohol. Evidence may be any information about the fact obtained in accordance with the procedures prescribed by law and confirmed in a certain procedural form.[123]

- *Must such evidence be examined by an expert witness?*

No, it is clear from the case-law that an expert opinion is subject to a plausibility assessment and does not have higher credibility than other evidence.[124] The Criminal Procedure Law does not provide for any specific case when a fact (circumstance) should be proved with a specific type of evidence or that in a particular situation it should be given a higher degree of reliability.[125]

- *If not obligatory, is this a common practice?*

[120] Commentary on Section 128 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 436.
[121] Section 128(3) of the Criminal Procedure Law.
[122] Commentary on Section 128 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 436.
[123] Supreme Court of the Republic of Latvia 19.09.2018. decision in criminal case No. 11331039917 (SKK477/2018). Available at: http://at.gov.lv/downloadlawfile/5604 [accessed 4 August 2020].
[124] Supreme Court of the Republic of Latvia 19.06.2008. decision in criminal case No. 1410058103 (SKK-258/2008). Available at: http://at.gov.lv/downloadlawfile/4070 [accessed 4 August 2020].
[125] Commentary on Section 128 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 436.

Depending on the situation. The more complex case with more electronic evidence, the more often expert opinions are used.

- *What are the requirements for experts (experience, independence, training, etc.)?*

The following natural person may be a forensic expert candidate:

1) who has acquired an accredited study programme corresponding to the speciality chosen in an institution of higher education;
2) who has acquired professional knowledge and experience of a forensic expert:
    a) in a forensic expert-examination institution or under supervision of a forensic expert by acquiring a training programme in the corresponding speciality of a forensic expert, and who has submitted an application for certification within two years after obtaining an attestation regarding the acquisition of the candidate training programme issued by a forensic expert-examination institution or a forensic expert,
    b) by obtaining a certificate of a medical practitioner in the main speciality of forensic medicine expert or sub-speciality of forensic psychiatry expert;
3) who is fluent in the official language at the highest level;
4) who has an impeccable reputation.[126]

A person whose professional activity is confirmed by a forensic expert certificate issued in accordance with the procedures specified in regulatory enactments in one of the specialties of a forensic expert may be a forensic expert.[127] A forensic expert should be independent in the performance of forensic expert-examination and preparation of an opinion.[128] His activities and

[126] Section 6(1) of the Law On Forensic Experts, *Latvijas Vēstnesis*, 42, 01.03.2016. Available at: https://likumi.lv/ta/en/id/280576-law-on-forensic-experts [accessed 4 August 2020].
[127] Section 1 point 2 of the Law On Forensic Experts.
[128] Section 14(1) of the Law On Forensic Experts.

conclusions should not be influenced by the head of the expert institution or the person directing the particular criminal proceedings.[129]

- *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?*

No, there is only the Office for Combating Economic Crimes. It is a structural unit of the Main Criminal Police Department of the State Police, which deals with the investigation of the most complex economic crimes in the country, including cybercrime. Criminal cases involving mobile forensics are mainly investigated by this police unit.

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

**Answer:**

No, unfortunately, there is no case law available in a publicly available database of court decisions regarding interpretation and presentation of evidence produced using mobile forensics.

***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:**

[129] Commentary on Section 33 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 138.

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

No, there are only general rules. Please look at the answer to question 40.

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

**Answer:**

No, unfortunately, there is no case law available in a publicly available database of court 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:**

No, there are no rules, guidance, or case law in Latvia on how to respect the right to a fair trial in case of evidence extracted via mobile forensics. In this case, the general rules on the right to a fair trial and equality are taken into account. For example, the Criminal Procedure Law determine a uniform procedural order for all persons involved in criminal proceedings irrespective of the origin, social and financial situation, employment, citizenship, race, nationality, attitude toward religion, sex, education, language, place of residence, and other conditions of such persons.[130]

In a court hearing, an accused, his/her representative and defence counsel, a victim and his/her representative, as well as the owner of property affected during criminal proceedings whose property has been seized, and a prosecutor **have equal rights to** submit recusals, submit requests, submit evidence, indicating why they had not been submitted to a court hitherto, participate in verification of evidence, submit written explanations to the court, participate in court debates, and to participate in the trial of other matters that have arisen during the course of a criminal case.[131]

***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 law does not require training for the judges, prosecution, expert witnesses, lawyers regarding evidence coming from mobile forensics. Although, such training on electronic evidence for judges,

[130] Section 8 of the Criminal Procedure Law.
[131] Section 455(1) of the Criminal Procedure Law.

investigators and prosecutors takes place, especially in later years. During such training, judges and prosecution acquire knowledge about electronic evidence and the challenges associated with it. For example, investigators are given the opportunity to learn investigative analysis tools and discuss the consequences of a failed analysis. Judges and prosecutors, in turn, gain knowledge of digital evidence, encrypted data and cryptocurrencies.

When the e-Evidence platform developed by the European Commission was launched in 2019, in Latvia, there were also planned some training for officials of the involved institutions (prosecutor's office, police, courts) in the use of the e-Evidence 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:**

No, an inspection is not limited in time by law. It can be performed as long it is necessary. However, each person has the right to the completion of criminal proceedings within a reasonable term, that is, without unjustified delay. The completion of criminal proceedings within a reasonable term is connected with the scope of a case, legal complexity, amount of procedural activities, attitude of persons involved in the proceedings towards fulfilment of duties and other objective conditions.[132]

***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:**

Latvian regulation does not separate the procedural rights inherent to the different participants in a criminal procedure regarding the use of mobile forensics. Therefore, the answer to this question provides general rules to the different participants in a criminal procedure.

[132] Section 14(1) of the Criminal Procedure Law.

The prosecution:

1) In some cases, a prosecutor also can decide the question regarding the commencement of criminal proceedings and can conduct investigations himself/herself.[133]
2) The prosecutor supervising an investigation has the right to:
    - take a decision to initiate criminal proceedings and to transfer them to an investigating institution;
    - give instructions and request execution of the provided instructions;
    - carry out investigative actions, informing the person directing the proceedings beforehand regarding such carrying out of investigative actions;
    - familiarise himself/herself at any time with the materials of the criminal proceedings;
    - revoke the decisions of the person directing the proceedings and a member of the investigative group, and also the decisions of the direct supervisor of the investigator which are not related to organisational issues of significance to the proceedings.[134]
3) A supervising prosecutor acquires the status of the person directing the proceedings from the moment when he/she takes over the leadership of criminal proceedings and decides on the initiation of criminal proceedings.[135] In that case the prosecutor as a person directing the proceedings has the right in criminal prosecution:
    - to terminate criminal prosecution and to determine additional investigation;
    - to take any procedural decision in accordance with the procedures laid down by the law and to perform any procedural action or assign the performance thereof to a member of an investigative group or the executor of procedural tasks;
    - to terminate criminal proceedings, applying the prosecutor's penal order;

[133] Section 36(2) of the Criminal Procedure Law.
[134] Section 37(3) of the Criminal Procedure Law.
[135] Section 38(1) of the Criminal Procedure Law.

- to prepare an draft agreement;
- to submit proposals for the recognition of specified facts as proven without an verification of evidence in a court
- if necessary, to request an evaluation report of a person from the State Probation Service.[136]

4) The prosecutor has the right to request to read or play in a court hearing fully or partially written evidence, which is related to the object of evidence.[137]
5) The prosecutor has rights to submit recusals, submit requests, submit evidence, indicating why they had not been submitted to a court hitherto, participate in the verification of evidence, submit written explanations to the court, participate in court debates, and to participate in the trial of other matters that have arisen during the course of a criminal case.[138]
6) In order to submit additional evidence, a prosecutor has the right in the trial to request documents of importance to the criminal proceedings and information regarding facts from natural persons and legal persons, **except data stored in an electronic information system from the merchant of this system**.[139] In the trial, the judge or the court panel only may request that.[140]

The court:

1) Written evidence, which is related to the object of evidence, should be read or played in a court hearing fully or partially, if the person who conducts defence, a prosecutor, a victim or his/her representative, and the owner of the property affected during criminal proceedings whose property has been seized has applied such request.[141]

[136] Section 39(2) of the Criminal Procedure Law.
[137] Section 449(3) of the Criminal Procedure Law.
[138] Section 455(1) of the Criminal Procedure Law.
[139] Section 455(1[1]) of the Criminal Procedure Law.
[140] Section 192(3) of the Criminal Procedure Law.
[141] Section 449(3) of the Criminal Procedure Law.

2) The written evidence indicated in a decision to transfer a criminal case to a court should be examined in a court hearing only when the person who conducts defence, a prosecutor, a victim or his/her representative and the owner of property infringed during criminal proceedings whose property has been seized has submitted such a request.[142]
3) If a request is justified, a court decides on an inspection of material evidence.[143]
4) A court may decide on non-conducting of verification of evidence in relation to an entire prosecution or the independent part thereof only provided that:
    - the accused admits his/her guilt in the entire prosecution directed against him/her or in the relevant part thereof;
    - the court does not have any doubts regarding the guilt of the accused after an examination of case materials;
    - the accused, or, in cases of mandatory defence, also his/her defence counsel and representative, agrees to the non-conducting of such examination.
5) If the information obtained in operational activities measures is used in a criminal case as evidence, only the court upon a reasoned request of the prosecutor, victim, accused or his/her defence counsel may become acquainted with the materials of operational activities, which are not appended to the criminal case and are related to the object of evidence, indicating in the case materials and ruling that such materials have been evaluated.[144]
6) A court is entitled to acquire evidence on the basis of the initiative thereof, and to examine such evidence in a court hearing, only in the case where the accused conducts defence himself/herself, and justified doubts arise for the court regarding his/her mental capacity or possible guilt in the prosecution.[145]

The defendant:

[142] Ibid.
[143] Section 449(4) of the Criminal Procedure Law.
[144] Section 500(4) of the Criminal Procedure Law.
[145] Section 455(2) of the Criminal Procedure Law.

1) The person who conducts defence may request to read or play in a court hearing fully or partially written evidence, which is related to the object of evidence.[146]
2) The accused and defence have rights to submit recusals, submit requests, submit evidence, indicating why they had not been submitted to a court hitherto, participate in the verification of evidence, submit written explanations to the court, participate in court debates, and to participate in the trial of other matters that have arisen during the course of a criminal case.[147]

The victim:

1) The victim may request to read or play in a court hearing fully or partially written evidence, which are related to the object of evidence.[148]
2) The victim has rights to submit recusals, submit requests, submit evidence, indicating why they had not been submitted to a court hitherto, participate in the verification of evidence, submit written explanations to the court, participate in court debates, and to participate in the trial of other matters that have arisen during the course of a criminal case.[149]

## 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:**

Procurators follow the requirements stated by the Criminal Procedure Law and other laws, and they do not have some specific guidance provided. As prosecutors also have a variety of training, including on electronic evidence, they gain knowledge of the rules on how to control and deal with

[146] Section 449(3) of the Criminal Procedure Law.
[147] Section 455(1) of the Criminal Procedure Law.
[148] Section 449(3) of the Criminal Procedure Law.
[149] Section 455(1) of the Criminal Procedure Law.

mobile forensics and evidences. When dealing with mobile forensics, prosecutors also follow current practice and experience.

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**:

In any case, the main primary duty of the court is to examine the evidence and to base the court's decision on the assessment of the information mentioned in the evidence. In court, the examination of evidence takes the form of a debate between the parties, providing an assessment of the evidence and substantiating its conclusions and allegations. The Criminal Procedure Law gives the court the right to assess whether the approaches and methods used for acquiring, collecting and analyzing evidence have been properly applied.

Tiesa pārbauda, vai pierādījumi ir iegūti likumā paredzētajā kārtībā un nostiprināti likumā noteiktā procesuālajā formā.[150] The court examines whether the evidence has been obtained in accordance with the procedure prescribed by law and fixed in specific procedural form prescribed by law.[151] This means that there is judicial control over the approaches and methods used for acquiring, collecting and analyzing evidence in accordance with the Criminal Procedure Law.

***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:**

The court examines all electronic evidence. Although, for example, video, photo and audio evidence can be perceived and assessed by the court itself, but if electronic evidence is more

[150] Section 127(1) of the Criminal Procedure Law.
[151] Section 127(1) of the Criminal Procedure Law.

complex and requires special knowledge obtain it, an expert is called in and then the court assesses such evidence based on the expert's explanations.

Although the case law do not illustrate how the court assess the evidence obtained via mobile forensics, looking from more technical point of view, the court correctly assesses the evidence but in judgment the terms of these evidences are used improperly. In practice, there are different interpretations of the status of electronic information media. According to the regulation, the status of electronic information or "computerised information media" in criminal proceedings is a "document" because it is used in evidence due to the information contained therein.[152] Also, if a thing (material evidence) is to be used in evidence due to the substantive information contained therein, it is considered not as material evidence, but as a document.[153] However, the electronic media is often used as material evidence in criminal proceedings. For example, in some cases, hard drives, CD and DVD matrices, USB flash drives, mobile phones, laptops and SIM cards have been found to be material evidence.[154] Of course, sometimes it may also be used as material evidence because of its material characteristics, such as the fingerprints found on it. However, in these criminal cases found in case law, all the listed things were used in evidence due to the substantive information they contained.

Regulation states that recordings made with sound- and image-recording technical means are also considered as documents, within the meaning of evidence, in criminal proceedings.[155] Although, in some cases video surveillance recordings are recognised as electronic evidence.[156]

[152] Section 135(2) of the Criminal Procedure Law.
[153] Section 134(2) of the Criminal Procedure Law.
[154] Riga District Court 22.05.2019. judgment in criminal case No. 11816012917. Available at: https://manas.tiesas.lv/eTiesasMvc/nolemumi/pdf/384594.pdf [accessed 4 August 2020]; Riga District Court 11.09.2019. judgment in criminal case No. 11816011718. Available at: https://manas.tiesas.lv/eTiesasMvc/nolemumi/pdf/391271.pdf [accessed 4 August 2020]; Vidzeme District Court 09.11.2018. judgment in criminal case No. 11130039418. Available at: https://manas.tiesas.lv/eTiesasMvc/nolemumi/pdf/378889.pdf [accessed 4 August 2020].
[155] Section 135(2) of the Criminal Procedure Law.
[156] Rezekne court 26.09.2019. judgment in criminal case No. 11110033318. Available at: https://manas.tiesas.lv/eTiesasMvc/nolemumi/pdf/392007.pdf [accessed 4 August 2020].

There are also cases when the same data carrier is referred to differently in the decision. For example, in a judgment, CD with video recording is referred to as both electronic evidence and material evidence.[157] The database of anonymised rulings also contains decisions, where the status of the data carrier is determined precisely. For example, in one case, a DVD-R disc with information from a merchant of electronic communications and a CD-R disc are called documents.[158] However, in most cases, data carriers are mentioned as material evidence in criminal judgments.

## 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**:

A defence counsel has all the rights that are held by his/her defendant in the relevant proceedings, as well as the right to familiarise himself/herself, after completion of pre-trial criminal proceedings, with the materials of a criminal case, and to copy the necessary materials with technical means.[159]

An accused has the same rights in pre-trial criminal proceedings as a suspect, as well as the rights after completion of pre-trial criminal proceedings, to receive copies of all the materials of a criminal case to be transferred to a court, which relate to the accusation brought against him/her and his/her

[157] Gulbene District court 02.02.2017. judgment in criminal case No. 11170017316. Available at: https://manas.tiesas.lv/eTiesasMvc/nolemumi/pdf/299939.pdf [accessed 4 August 2020].
[158] Riga District court 04.01.2018. judgment in criminal case No. 11351012415. Available at: https://manas.tiesas.lv/eTiesasMvc/nolemumi/pdf/341864.pdf [accessed 4 August 2020].
[159] Section 86(1) point 4 of the Criminal Procedure Law.

personality, if such materials have not been issued earlier or with the consent of a prosecutor to become acquainted with these materials.[160]

Although the defence counsel has the right to copy the necessary materials by technical means, in practice the exercise of this right is usually not necessary, as the accused has the right to receive copies of the criminal case file in paper[161], so they are also available to the defence counsel. If the defense counsel needs electronic evidence (for example, electronic data) from the case file, then such a request, which should be justified, must be submitted to the court. The court considers the request and unfortunately does not always satisfy it.

Additional copying of criminal case materials may be necessary only in cases where the prosecutor has considered that part of the criminal proceedings material does not relate to the charge against the defendant and has not provided the accused with copies of the case file in this part, but the defence counsel considers these materials necessary for defence.[162] As the question is regarding procedural issues that are not reflected in the judgments available in the public database, we cannot refer to case law.

## 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:**

[160] Section 70(1) point 1 of the Criminal Procedure Law.
[161] Section 70(1) point 1 of the Criminal Procedure Law.
[162] Commentary on Section 86 of the Criminal Procedure Law. In: Krimināprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 301.

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

In pre-trial criminal proceedings, a witness provides information in an inquiry or interrogation. During trial, a witness provides information only in an interrogation.[163] A witness has the right to know in what criminal proceedings he/she has been invited to testify, to which official he/she has provided information, and the procedural status of such official.[164]

A witness has the right:

1) to make notes and additions in testimonies recorded in writing;[165]
2) to not testify against himself/herself or against his/her immediate family[166] (the betrothed, spouse, parents, grandparents, children grandchildren, brothers or sisters of such person, as well as of the person with whom the relevant natural person is living together and with whom he/she has a common (joint) household)[167];
3) to submit a complaint to an investigating judge regarding the unjustified disclosure of a private secret, or to request that the court withdraws a matter regarding a private secret, and to request that the request is entered in the minutes of the court hearing if such request is rejected[168] (in turn, in court for this reason, the witness is entitled to ask the court to withdraw the questions of privacy and to request that the request be recorded in the minutes of the court hearing, if it is rejected[169]).

An image of a witness recorded as a photograph, video, or by other types of technical means should not be published in the mass media during procedural actions without the consent of such witness if such publication is not necessary for the disclosure of a criminal offence.[170]

[163] Section 109(2) of the Criminal Procedure Law.
[164] Section 110(1) of the Criminal Procedure Law.
[165] Section 110(3) point 1 of the Criminal Procedure Law.
[166] Section 110(3) point 2 of the Criminal Procedure Law.
[167] Section 12(5) of the Criminal Procedure Law.
[168] Section 110(3) point 4 of the Criminal Procedure Law.
[169] Commentary on Section 110 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 375.
[170] Section 110(4) of the Criminal Procedure Law.

Witnesses may be interrogated regarding all the circumstances and regarding any person involved in the criminal proceedings if the information provided is or may be significant in a case.[171] What a witness may and can be testify about is extensive. This is any information relevant to the criminal proceedings (circumstances, persons, etc.).[172]

## 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:**

A victim has the following rights:

- to receive information regarding the conditions for applying for and receipt of a compensation, including State compensation and to submit an application regarding compensation for the harm inflicted in accordance with the procedures laid down in this Law;
- to participate in criminal proceedings, using the language in which he or she is fluent, if necessary, using the assistance of an interpreter without remuneration;
- to settle with a person who has inflicted harm to him or her, as well as to receive information regarding implementation of the settlement and its consequences;
- to invite an advocate for the receipt of legal assistance;
- to submit an application for taking measures in case of a threat to the person himself or herself, his or her immediate family or property;

[171] Section 151(2) of the Criminal Procedure Law.
[172] Commentary on Section 151 of the Criminal Procedure Law. In: Kriminālprocesa likuma komentāri. A daļa. Zinātniska monogrāfija prof. Kristīnes Stradas-Rozenbergas zinātniskā redakcijā. Rīga: Latvijas Vēstnesis, 2019, p. 495.

- in the cases provided for in this Law to submit an application regarding reimbursement of procedural expenses which have arisen during criminal proceedings;
- to submit a complaint in the cases, within the terms and in accordance with the procedures laid down in this law regarding a procedural ruling or an action of an official authorised for the conduct of criminal proceedings;
- to receive contact information for communication regarding the particular criminal proceedings;
- to receive information regarding the support and medical assistance available;
- to request information regarding the direction of the criminal proceedings, regarding the officials who conduct or have conducted criminal proceedings.[173]

A victim's privacy is preserved by the rights to not testify against himself/herself or against his/her immediate family.[174] Although, if a victim refused to provide testimony and he/she was informed regarding such right, but nevertheless did provide such testimony, then such testimony should be assessed as evidence.[175]

A victim as any other person involved in criminal proceedings can use the evidence obtained via mobile forensics when exercising their rights.

[173] Section 97.[1](1) of the Criminal Procedure Law.
[174] Section 97.[1](1) point 3 of the Criminal Procedure Law.
[175] Section 131(3) of the Criminal Procedure Law.

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

## Section 6: Comments

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

**Answer:**

Unfortunately, Latvian regulation, court and police practice regarding mobile forensic tools and evidence is very limited. It is still in its infancy, so many issues are covered by the general regulation on electronic evidence in accordance with the Criminal Procedure Law.