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

Contents

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,

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

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.

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.

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

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?*

University of Zagreb Faculty of Law, Associate Professor

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

Zagreb, Croatia

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)*

There is no legally defined term for a mobile device in the Croatian national system. However, smartphones, tablets and other similar modern mobile devices fit into the concept of a "computer system" in Article 87, point 18 the Croatian Criminal Code[1], which was enacted in line with the Council of Europe Cybercrime Convention. Namely, a computer system is defined as "any device or a group of inter-connected or inter-linked devices, one or more of which process data automatically on the basis of a program, as well as computer data stored or processed in, read or transferred into it for the purpose of its operation, use, protection and maintenance." This interpretation is supported by relevant Guidance of the Cybercrime Convention Committee.[2] There is also case law confirming this in Croatian judicial practice.[3]

[1] Article 87, point 18 of the Criminal Code (title in original language: Kazneni zakon), Official Gazette no. 125/11, 144/12, 56/15, 61/15, 101/17, 118/18 and 126/19.
[2] T-CY Guidances Notes, 15.11.2016, T-CY(2013)29rev, https://rm.coe.int/16806c79dd.
[3] Supreme Court of the Republic of Croatia, judgment, III Kr 32/08-3, 29.10.2008.

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

Researcher's overview

Preliminary notes:

a) Note on case law in the questionnaire: many decisions covered relate to claims on exclusion of evidence, with main proceedings still ongoing and/or final court decisions in the case not being final yet
b) Note on translated text into English: mainly done by researcher (where available, unofficial translations of acts were used)

Electronic evidence in the CPA (and related provisions)

Electronic (digital) evidence is defined as data, which was obtained as evidence in electronic (digital) form under the CPA (Article 202, paragraph 2, item 33). Unless prescribed otherwise in the CPA, electronic evidence is obtained (collected) by applying provisions of Articles 257 on search of a movable, and provisions of Articles 262 and 263 on the temporary seizure of objects (Article 331).

Search of a Movable (Article 257)

(1) A search of movables shall also include a search of a computer and devices connected therewith, of other devices intended for collecting, saving and transferring data, for telephone, computer and other kinds of communication, and of data carriers. At the request of the authority conducting a search, the person using a computer or having access to a computer or another device or data carrier, as well as a telecommunications service provider shall enable access to a computer, device or data carrier and shall provide the necessary information for unhindered use and achievement of the goals of the search. (2) Upon the order of the authority carrying out a search, the person using a computer or having access to a computer and other devices referred to in paragraph 1 of this Article, and a telecommunications service provider, shall immediately take measures to prevent the destruction or modification of data. The authority carrying out a search may order that an expert assistant take these measures. (3) The person using a computer or having access to a computer or other device or data carrier, and a telecommunications service provider, who does not comply with the requirements of paragraphs 1 and 2 of this Article, despite there being no justifiable reasons therefore, may, upon the motion of the State Attorney, be punished by the judge of investigation in accordance with the provision of Article 259, paragraph 1, of this Act. The provision on punishment shall not apply to the defendant.

Search: Common provisions (CPA)

Article 240
(1) Search means an examination of the object of the search by means of senses and their aids under the conditions and in the manner prescribed by this Act and other regulations. (2) The search of a home, other premises, means of transport, any other movable or a person shall be conducted for the purpose of finding the perpetrator of a criminal offence, an object or traces important for criminal proceedings, where it is

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

probable that they are located in a specific place, in the immediate surroundings of or on a certain person.(3) Search regulations shall not apply to natural, public or abandoned premises.

Article 242

(1) Unless otherwise prescribed by this Act, at the request of the State Attorney the judge of investigation shall order a search by a written warrant including a statement of reasons. The search warrant shall contain the following:
1) designation of the object of search (person, home, other premises or movables); 2) purpose of the search; 3) authority conducting the search.
(2) The judge of investigation shall decide on the request for search as soon as possible, but not later than four hours from the receipt of the request. Should the judge of investigation deny the request, he or she shall issue an order. The State Attorney shall be entitled to appeal against the order of the judge of investigation within the time limit of eight hours. Any appeal shall be decided by the panel within the time limit of twelve hours. (3) The search warrant issued by the judge of investigation and referred to in paragraph 1 of this Article shall be executed within the time limit of three days from the date of its issue. After the expiry of the said time limit, a search may no longer be conducted on the basis of the said warrant. The warrant shall be immediately returned to the judge of investigation who shall make a note on it invalidating it. (4) A search shall be conducted by the State Attorney, the investigator or the police. (5) Where the investigation is conducted by the judge of investigation, he shall designate in the search warrant the investigator who is to conduct the search. The investigator shall conduct the search as stipulated in the warrant and shall immediately deliver to the judge of investigation the minutes of the search and the objects that were temporarily seized.

Article 243

(1) Unless otherwise prescribed by this Act, before a search starts, the search warrant shall be handed to the person whose premises will be searched or who will be searched, or to the person who is in possession of the object of the search. (2) Before the start of the search, the person referred to in paragraph 1 of this Article shall be invited to voluntarily hand over the person or objects searched for.

Article 244

By way of exception, a search may be commenced even without the prior handing of a warrant (Article 243, paragraph 1) and the instruction on rights (Article 239, paragraph 1), or an invitation to hand over a person or objects (Article 243, paragraph 2) where: 1) armed resistance is expected; 2) it is necessary that a surprise search be conducted due to suspicion that criminal offences were committed by a group or criminal organisation, or a criminal association or that the criminal offences were committed as part of a criminal association, or that their perpetrators have links with persons abroad, 3) a search of public premises is to be conducted; 4) it is suspected that a prior warning would enable the hiding or destruction of or damage to objects or traces that need to be seized; 5) it is suspected that a prior warning would endanger the safety of the person conducting the search; 6) the owner or possessor of a home or movable is unavailable.

Urgent search of a person and means of transport (Article 245)

1) By way of exception, where a search must be conducted immediately because its postponement would put at risk the achievement of the goals of the search, the State Attorney himself or herself may issue a written reasoned warrant ordering the search of a person and means of transport, where there is a suspicion that the following criminal offences from the Criminal Code have been committed: criminal offences against humanity and human dignity (Title IX) punishable by imprisonment for a term exceeding five years, murder (Article 110), aggravated murder (Article 111), kidnapping (Article 137, paragraphs 2 and 3), unlawful deprivation of liberty (Article 136, paragraphs 3 and 4), unauthorised manufacture of and traffic in illicit drugs (Article 190, paragraphs 2, 3, 4 and 5), unauthorised manufacture of and traffic in substances banned in sports (Article 191a, paragraphs 2, 3 and 4), money laundering (Article 265), counterfeiting money (Article 274), taking a bribe (Article 293), giving a bribe (Article 294), receiving bribes in business dealings (Article 252), giving bribes in business dealings (Article 253), giving a bribe for trading in influence (Article 296), receiving or giving bribes during bankruptcy proceedings (Article 251), criminal association (Article 328), committing a criminal offence as a member of a criminal association (Article 329), disclosure of secret information (Article 347, paragraphs 1 and 4), espionage (Article 348, paragraphs 3, 4 and 5), murder of an internationally protected person (Article 352), kidnapping of an internationally protected person (Article 353), and criminal offences committed by a criminal association or criminal offences committed in concurrence by persons acting as members of a criminal association.
(2) The search referred to in paragraph 1 of this Article shall be conducted in compliance with Article 244. of this Act. (3) The State Attorney shall deliver the search warrant referred to in paragraph 1 of this Article together with the minutes of the conducted search to the judge of investigation as soon as possible, but no later than eight hours after the completion of the search. (4) The judge of investigation shall decide by an order on the legality of the State Attorney's search warrant and the conducted search within the time limit of eight hours from the receipt of the minutes. The State Attorney shall be entitled to file an appeal against the order of the judge of investigation denying the certification of the search warrant or the minutes of the conducted search within the time limit of twenty-four hours. Any appeal shall be decided by the panel within the time limit of forty-eight hours.

Search without a warrant - inspection, police search of a home without a warrant, including to find or secure evidence (Article 246)

(1) The State Attorney, the investigator or the police conducting inspection of the scene of commission of a criminal offence prosecuted ex officio may conduct a search without a warrant immediately and no later than eight hours after the criminal offence is detected, if that is absolutely necessary for averting a danger to the lives and health of people or to property of considerable value or for securing any traces or evidence directly related to the criminal offence giving rise to the inspection, unless the search in question is a search of the home or premises referred to in Article 256 of the present Act. (2) The police may conduct a search of a home or other premises in the absence of a search warrant: 1) where it is authorised by a special act to enter a person's home or other premises, provided that the requirements referred to in Article 240, paragraph 2, of this Act have been complied with; 2) where this is absolutely necessary for the purpose of executing an arrest warrant or arresting the perpetrator of a criminal offence (Article 107, item 2) punishable by imprisonment for a term of at least three years. (3) In the case of a search referred to in paragraph 2 of this Article, where a search of the home or other premises of the perpetrator is conducted, the said search can also be conducted for the purpose of finding or securing evidence. Such a search may be conducted only in the presence of at least two witnesses. (4) The police may conduct a search of a

person without a search warrant when executing a warrant for someone's bringing in or on the occasion of an arrest, if it is probable that the said person is in possession of offensive weapons or tools or that he or she will discard, hide or destroy objects or traces that need to be seized from him or her and used as evidence in proceedings. (5) When the police conducts a search in the absence of a search warrant, it shall immediately deliver the protocol of the search and the report to the State Attorney having jurisdiction.

Article 247

(1) A search is conducted during the daytime, from six o'clock in the morning to nine o'clock in the evening. (2) A search may be conducted at night only where there is a risk of delay, if: 1) it started in the daytime but was not finished; 2) the search in question is a search under Article 245, paragraph 1, and Article 246 of the present Act. (3) A search may be conducted at night if the person at whose place the search is conducted or that is being searched requests so himself, which shall immediately be entered in the minutes of the search and signed by the person in question. (4) The judge of investigation may, at the State Attorney's written reasoned request, allow a search to be conducted outside the period of time referred to in paragraph 1 of this Article also where it is probable that: 1) the objects or traces searched for will be destroyed or concealed; 2) the person searched for will hide or escape; 3) the person searched for will commit a criminal offence; 4) the safety of persons will be put at risk if the search is not conducted outside the period of time referred to in paragraph 1 of this Article.

Article 248

(1) Minutes shall be made of every search, which shall be signed by the person searched or the person whose premises are searched as well as by the persons whose presence during the search is mandatory. A copy of the minutes shall be given to the person searched or the person whose premises were searched. (2) Only such objects and documents that are related to the purpose of a search, as well as the objects specified in Article 249, paragraphs 1 and 2, of this Act shall be temporarily seized during the search.
(3) The minutes shall describe in detail the objects and documents seized, and this shall be entered in the receipt, a copy of which shall be issued immediately to the person from whom the said objects or documents have been seized.

Article 249

(1) If during a search objects not related to the criminal offence for which a search warrant was issued are found, however, which objects point to the commission of another criminal offence prosecuted ex officio, the said objects shall be described in the minutes and temporarily seized and a seizure receipt shall be immediately issued. The State Attorney shall be immediately notified thereof. (2) Where the State Attorney establishes that there is no ground for instituting criminal proceedings and where there is no other statutory ground for the seizure of the objects concerned, the said objects shall be immediately returned, of which minutes shall be drafted. The objects used during search of a computer and similar devices shall be returned to their users after the search, provided they are not necessary for the further conduct of criminal proceedings. (3) Personal data obtained by a search may only be used for the purposes of criminal proceedings and shall be erased without delay when this purpose ceases to exist.

Unlawful evidence obtained by search as well as minutes of search (Article 250)

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

The minutes of a search and the evidence obtained by a search cannot be used as evidence in proceedings, if:
1) search was conducted without a written search warrant in violation of this Act;
2) search without a warrant was carried out in violation of provisions of Article 246, paragraphs 1 to 3, of this Act;
3) the State Attorney failed to hand over the warrant and the minutes of the conducted search to the judge of investigation within the time limit referred to in Article 245, paragraph 3, of this Act;
4) request for the certification of a written search warrant of the State Attorney or of the minutes of the conducted search (Article 245, paragraph 4) has been denied;
5) circumstances due to which a search of a person was carried out by a person of the opposite sex were not entered into the minutes (Article 251, paragraph 2);
6) search was carried out in violation of the provisions of Article 251, paragraphs 3 and 4, of this Act;
7) search was carried out in the absence of the person required to be present during the search (Article 254, paragraph 2);
8) search was carried out in violation of conditions for legality of a search prescribed in a special act (Article 256).

Search of a person (Article 251) - includes also movables on him or in his posession

The search of a person shall include the search of the person's clothing, footwear, the exterior of his body, the movables on him or in his possession, the means of transport used by him at the time of the search and the premises at which the person happens to find himself at the time of the search, with the exception of his home.

Search of a home and other premises (Article 252) – includes search of movables if in search warrant or where conditions for a search without a warrant of the persons found there exist (252/3)

(1) A search of a home shall include a search of one or more spatially connected rooms used by a person as a home as well as of premises spatially connected with the home that are used for the same purpose.
(2) A search of other premises shall include a search of premises not used as a home that are designated in the search warrant, in which premises a search without a search warrant may not be carried out (Article 246, paragraph 2, items 1 and 2).
(3) A search of a home and other premises shall also include a search of movables and all the persons that happen to be in a home and on other premises, where this is stipulated in the search warrant or where conditions for a search without a warrant of the persons found there exist.

Article 253

(1) Prior to the start of a search of a home, the person to whom the search warrant refers shall be instructed on his or her right to notify a defence counsel who may be present during the search. (2) The authority carrying out a search shall allow this person to retain a defence counsel of his or her own choice and shall stop the search for this purpose until the arrival of the defence counsel but not for a period longer than three hours from the moment the person stated he or she wished to retain a defence counsel. If it is apparent from the circumstances that the retained defence counsel will not be able to arrive within the said

time limit, the authority carrying out a search shall allow a person to retain a defence counsel from the list of attorneys on call compiled by the Croatian Bar Association for each county territory and delivered to the State Attorney and the competent police administrations along with a report for the judge of investigation. The period during which the search of a home is suspended shall not be credited towards the statutory time limit set for a person's bringing in as referred to in Article 109, paragraph 2, of this Act. The authority carrying out the search shall note the period of suspension in the minutes of the search. (3) If a person does not retain a defence counsel or the retained defence counsel fails to appear within the said time limit, the authority may resume the search of a home.

Article 254

(1) A person who is in the possession of or resides on the premises or a person authorised by such a person to be present during a search may be present during the search of a home or other premises. (2) At least two citizens of age shall be present as witnesses during the search of a home or other premises. (3) Prior to the start of a search, witnesses shall be instructed to pay attention to how the search is conducted and shall be notified of their right to state their comments in the minutes of the search before they sign it if they deem that the search was not conducted in the manner prescribed by this Act or that the contents of the minutes are incorrect. (4) Where a search is conducted on the premises of a government body, a representative of the said body shall be invited to be present during the search. (5) Where a search is conducted on the premises of another legal entity, their representative shall be invited who may be present during the search.

Temporary Seizure, Articles 261-263

Article 261
(1) Objects that are to be seized under the Criminal Code or which may serve to establish facts in proceedings shall be temporarily seized and their safekeeping shall be ensured. (2) Whoever is in possession of such objects shall be required to hand them over at the request of the State Attorney, the investigator or the police. The State Attorney, the investigator or the police shall warn the holder of such an object of the consequences resulting from non-compliance with the request. (3) A person who for no justified reason fails to comply with the request to hand over objects may, upon a reasoned motion of the State Attorney, be punished by the judge of investigation pursuant to Article 259, paragraph 1 of this Act. (4) The measures referred to in paragraph 2 of this Article shall apply neither to the defendant nor to the persons exempt from the duty to testify (Article 285).

Article 262
(1) Temporary seizure shall not apply to:
1) files and other documents of government bodies, the publication of which would violate the confidentiality obligation until the competent authority decides otherwise; 2) written communication of the defendant to the defence counsel, unless the defendant requests otherwise; 3) recordings and private diaries found in the possession of persons referred to in Article 285, paragraph 1, items 1 through 3, of this Act, that were recorded or written by these persons and that contain recordings of or notes on facts about which these persons are not under a duty to testify; 4) notes, registry excerpts and similar documents in the possession of persons referred to in Article 285, paragraph 1, item 4, of this Act containing facts that these persons learned from the defendant in the performance of their professional duties; 5) notes on facts made

by journalists and editors in the media regarding sources of information and data disclosed to them in the performance of their professional duties, which were used in the media editing process and which are in their possession or in the possession of the editorial office for which they are employed.
(2) The ban on the temporary seizure of objects, documents and recordings referred to paragraph 1, items 2 through 5, of this Article shall not apply: 1) to a defence counsel or a person exempt from the duty to testify under Article 285, paragraph 1, of this Act where it is probable that they assisted the defendant in the commission of a criminal offence, assisted him after the commission of a criminal offence or acted as accessories after the fact; 2) to journalists and editors in the media if it is probable that they assisted the defendant in committing a criminal offence or assisted the defendant after he committed a criminal offence or that they acted as accessories after the fact, or to the criminal offences referred to in Articles 305 and 305a of the Criminal Code (Official Gazette 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08, 57/11 and 77/11) or to the criminal offences referred to in Articles 307 and 308 of the Criminal Code; 3) if the objects in question are to be seized under the law.
(3) Until the preferment of the indictment, the judge of investigation shall, at the request of the State Attorney, decide by an order on the probability of providing assistance in the criminal offence referred to in paragraph 2 of this Article. The judge of investigation shall issue an order within the time limit of 24 hours from the submission of the request by the State Attorney. Any appeal against the order of the judge of investigation shall be decided by the panel. After the preferment of the indictment, the court before which the proceedings are conducted shall render a decision. No appeal against the decision of the indictment panel and the trial court shall be allowed.
(4) The ban on the temporary seizure of objects, documents and recordings referred to in paragraph 1, items 2 through 5, of this Article shall not apply to cases concerning criminal offences of penal protection of children.
(5) The State Attorney, the investigator or the police may seize objects under paragraphs 1, 2 and 3 of this Article also when conducting inquiries into criminal offences or when the investigator or the police are executing a court warrant.
(6) Upon seizing an object, it shall be noted in the minutes where the object in question was found, the object shall be described and, where necessary, the establishment of its identity shall also be ensured in some other way. A receipt shall be issued for temporarily seized objects.
(7) An object seized in violation of the provisions of paragraph 1 of this Article cannot be used in evidence in criminal proceedings.

Temporary seizure of data stored in computers and devices connected thereto, as well as in devices used for collecting and transferring data, data carriers and subscription information in the possession of a service provider (Article 263)

(1) The provisions of Article 261 of this Act shall also apply to data stored in computers and devices connected thereto, as well as in devices used for collecting and transferring data, to data carriers and to subscription information in the possession of a service provider, except in cases where temporary seizure of objects is prohibited under Article 262 of this Act. (2) The data referred to in paragraph 1 of this Article must be handed over to the State Attorney at his written request in an integral, original, legible and understandable form. The State Attorney shall state in his request the time limit for the handing over of data. In the case of refusal to hand over data, it may be proceeded in accordance with Article 259, paragraph 1, of this Act. (3) The data referred to in paragraph 1 of this Act shall be recorded in real time

by the authority taking the action. In acquiring, recording, protecting and storing of data special attention shall be paid to rules on the confidentiality of certain data (Articles 186 through 188).[4] Depending on the circumstances, data that are not related to the criminal offence for which proceedings are undertaken, but which are needed by the person against whom the measure in question has been taken, may be recorded onto an appropriate medium and returned to this person also prior to the conclusion of proceedings. (4) Upon a motion of the State Attorney, the judge of investigation may decide by an order that all computer data referred to in paragraph 1 of this Article be preserved and safeguarded for as long as necessary, but not exceeding a period of six months. Afterwards the computer data shall be returned unless: 1) they concern the commission of criminal offences against computer systems, programmes and data (Title XXV) of the Criminal Code; 2) they are related to the commission of another criminal offence prosecuted ex officio, which was committed by means of a computer system; 3) they are to be used as evidence of a criminal offence for which proceedings are ongoing. (5) The person using the computer and the service provider are entitled to file an appeal against the order of the judge of investigation imposing the measures referred to in paragraph 3 of this Article within the time limit of twenty-four hours. The appeal shall be decided by the panel within the time limit of three days. The appeal shall not stay the execution of the order.

Article 264

(1) Government authorities may refuse to disclose or hand over their files and documents if these files and documents contain information considered confidential under a special act (classified information).

[4] Note: According to the Report on Croatia for the Council of the EU on fight against cybercrime, in connection with the data obtained under Article 263: "the complete recording and documentation shall be sealed and kept in the State Attorney's Office", in line with Article 338, paragraph 2 of the CPA (below). Council of the EU, Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime"- Report on Croatia, 5250/1/17, REV 1 DCL 1, GENVAL3 CYBER9, 11.4.2017, https://data.consilium.europa.eu/doc/document/ST-5250-2017-REV-1-DCL-1/en/pdf, p. 51. That provision, as enacted in the CPA, falls under the relevant section on special evidentiary measures in Article 332. While, logically, the stated measure (Article 338/2) should apply *per analogiam* also in cases of seizure of computer data specified in Article 263, fact is that currently no CPA provisions are explicitly and specifically designated for the cases of computer data seizure. See also provisions of Articles 267, 269 and 270 of the CPA.
Article 338 of the CPA: (1) The recordings, documents and objects obtained through the actions referred to in Article 332, paragraph 1, of this Act may be used in evidence only in proceedings against the person referred to in Article 332, paragraph 1, of this Act or in the case referred to in Article 335, paragraph 6, of this Act. (2) Recordings, transcripts and documentation shall be kept sealed in the State Attorney's Office in their entirety. Where circumstances allow, the judge of investigation shall order, upon the motion of the State Attorney, that only those parts of a recording, transcript and documentation which refer to the criminal proceeding in question be included in the case file. (3) For this purpose the State Attorney shall serve on the judge of investigation a motion which includes a statement of reasons and the full version of the recording which the judge of investigation shall return after the part of the recording which refers to the criminal proceedings in question is singled out. The singling out shall be made by an expert assistant under the supervision of the judge of investigation. (4) The State Attorney shall enable the defendant immediately upon his request to reproduce a recording or inspect a transcript or documents. After the recording has been reproduced or the transcript or documents inspected, the defendant may propose at the trial that the recording, transcript or documents be reproduced or read out in full or in part.

(2) Legal persons may request that data relating to their business not be revealed.
(3) The decision on the declassification of data referred to in paragraph 1 of this Article shall be taken by the government authority at the request of the State Attorney or the court.
(4) The decision on the disclosure of data referred to in paragraph 2 of this Article shall be taken by the judge of investigation or the court before which the trial takes place upon a reasoned motion of the State Attorney. No appeal against the order of the court before which the trial takes place shall be allowed.

Article 265

(1) Where access to data considered to be a bank secret is denied, the court may, at the request of the State Attorney which includes a statement of reasons, issue an order for the provision of these data. The court shall specify in the order the time limit by which the bank must provide the data.
(2) Where it is probable that a certain person receives into, holds or otherwise has at his disposal in his bank accounts proceeds of a criminal offence, which proceeds are important for the investigation of the criminal offence in question or are subject to forcible seizure under the law, the State Attorney shall propose to the court by a reasoned motion that it order the bank to provide data on the said accounts and proceeds to the State Attorney. The motion shall include data on the legal or natural person holding or having at its disposal these assets or proceeds. The description of proceeds shall include the currency designation but not necessarily the exact amount where this amount is not known. The court shall state in its order the time limit by which the bank must proceed as specified […]

Article 267
(1) The files or documents which have been temporarily seized because they may be used in evidence shall be listed. Where this is not possible, the files or documents shall be placed in an envelope and sealed. The person from whom a file or document is temporarily seized may place his/her seal and signature on the envelope. (2) The envelope shall be opened by the State Attorney. While examining files or documents, care must be taken not to disclose their contents to unauthorised persons. A protocol of the opening of the envelope shall be made. (3) The person from whom the files or documents have been seized shall be summoned to be present at the opening of the envelope. If the said person does not respond to the summons or is absent, the envelope shall be opened, the files or documents examined and an inventory of them made in his absence.

Article 269
(1) Before the indictment is preferred, objects that are to serve as evidence shall be kept in a special room of the State Attorney's Office. Afterwards they shall be kept in a special room at the court building. By way of exception, where this is not possible, these objects shall be kept off the State Attorney's or court premises. (2) The authority conducting proceedings shall be in charge of supervising these objects. (3) The minister responsible for justice shall adopt regulations on the method of and conditions for the safekeeping of objects referred to in paragraph 1 of this Article.[5]

[5] Ordinance on the handling of found and seized objects (title in original language: Pravilnik o postupanju s pronađenim i oduzetim predmetima, Official Gazette no. 50/2012. Ordinance regulates the manner and conditions under which found or confiscated items are kept, which may serve in establishing the facts in criminal proceedings or as evidence until the indictment is filed ("Corpore delicti"). According to Article 11 of this Ordinance, at the request of the State Attorney, data stored in computers and devices connected thereto, as well as in devices used for

Article 270
(1) Temporarily seized objects shall be returned as soon as they are no longer necessary for the further conduct of the proceeding unless under the law they are subject to the provisions on seizure or where statutory reasons for applying the measure referred to in Article 266, paragraph 2, of this Act cease to exist. (2) The State Attorney and the court shall, ex officio, take care that the reasons for keeping temporarily seized objects have not ceased to exist.

Presentation of evidence (Article 430)

Unless otherwise prescribed by the CPA, evidence obtained by examining documents[6] or reproducing recordings[7] and *electronic evidence* shall be presented as set forth in Articles 329 through 331 of the CPA.

Collecting and presenting documentary evidence (Article 329; as regards Articles 267 and 269: see above)

(1) Documents that serve to establish facts shall be obtained and kept in application of the provisions of this Title, taking care not to damage or destroy any document and to preserve its contents in unmodified form. Where necessary, the authority conducting the proceedings shall, after having verified the document accordingly, make a copy of it and return the original to the person who submitted the document. (2) With regard to documents, it shall be proceeded as with other objects that are to be used in evidence (Articles 267 and 269). (3) Documentary evidence shall be presented by way of its reading or examination .

Collecting and presenting recording evidence (Article 330; as regards Articles 267 and 269: see above)

(1) A recording serving to establish facts shall be obtained in application of the provisions of this Title.
(2) With regard to a recording, it shall be proceeded as with other objects that are to be used in evidence (Articles 267 and 269), taking care not to damage or destroy the recording and to preserve its contents in unmodified form. Where necessary, appropriate measures shall be taken in order to preserve the recording in unmodified form or to make a copy of it.
(3) Unless otherwise prescribed by this Act, the contents of a recording shall be established by reproduction. If the recording includes footage of a child, the recording shall be reproduced by modifying the image and the voice of the child where this is required for the purpose of protecting the interests of the child. In doing so, account shall be taken of the interests of the proceedings as a whole. (4) A recording shall be reproduced by an expert.

---

collecting and transferring data, must be handed over to the State Attorney, in accordance with the CPA. If, at the proposal of the State Attorney, the judge of investigation orders the protection and storage of computer data that have been temporarily seized, these data shall be kept in Corpora delicti for a maximum of six months, after which the computer data must be returned, unless otherwise provided by the CPA.

[6] Document shall mean any object containing a note (record), sign or picture that is suitable or has been designated to serve as evidence of some fact that is of relevance to legal relationships. Article 202, paragraph 2, item 28 of the CPA.

[7] Recording shall mean a record made by using a technical device. Article 202, paragraph 2, item 29 of the CPA.

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

Legality of electronic evidence / mobile device-data

Constitution of the Republic of Croatia prescribes that evidence obtained unlawfully may not be admitted in court proceedings (Article 29, paragraph 4). Under Article 10, paragraph 1 of the CPA, court decisions may not be founded on unlawfully obtained evidence (unlawful evidence), and that is evidence (Article 10, paragraph 2):

1) obtained in violation of the prohibition of torture, inhumane or degrading treatment provided for in the Constitution, statute or international law;
2) obtained in violation of the rights to defence, dignity, reputation and honour, and the rights to inviolability of personal and family life guaranteed by the Constitution, domestic or international law, except if such evidence was obtained in proceedings for grave forms of criminal offences falling within the jurisdiction of the county court[8] and with respect to which the interest of the perpetrator's criminal prosecution and punishment prevails over the violation of a right – however, in such cases the court decision may not be founded exclusively on such evidence (Article 10, paragraph 4 in connection with Article 10, paragraph 3 and Article 10, paragraph 2, item 2 of the CPA);
3) obtained in violation of criminal procedure provisions which is expressly provided for in the CPA (unlawful evidence ex lege);
4) of which knowledge has been gained from unlawful evidence ("fruit of the poisonous tree").

Not following applicable rules does not always lead to inadmissibility - it depends on what procedural rules had been violated. Under Article 10 of the CPA ex lege unlawful evidence is evidence obtained in violation of criminal procedure provisions which is expressly provided for in the CPA (e.g. violations of search rules as specified in Article 250; violations of Article 332 - per Article 335, paragraph 7 of the CPA; violations of rules on excluded objects for seizure - Article 262, paragraph 1 as per Article 262, paragraph 7; Article 263, paragraph 1 of the CPA; (unlawful) finding and opinion of a person who may not be appointed as expert witness (Article 311, paragraph 1 of the CPA). Also, it is evidence of which knowledge has been gained from unlawful evidence (e.g. minutes on search of the mobile phone represents unlawful evidence, where it became known from the unlawfully seized mobile phone, which may not be used as evidence in the proceedings - contravention of Article 250 of CPA, or, when object (mobile device / data) were seized in violation of Article 262, paragraph 1 (as per Article 262, paragraph 7; Article 263, paragraph 1 of the CPA). Shortcoming such as that minutes on seizure of a movable did not contain a note where the object was found (as prescribed by Article 262, paragraph 6 of the CPA[9]) did not in case law by itself render such evidentiary action unlawful. Also, acting contrary to Article 257, paragraph 2 of the CPA by not taking measures to prevent data destruction/ modification during search would not make evidence obtained unlawful per se, neither would the shortcomings/lacking in reasoning in the search warrant (not specified in Article 250 of the CPA).

[8] See Article 21 of the Act on the Office for the Suppression of Corruption and Organized Crime (USKOK), title in original language: Zakon o Uredu za suzbijanje korupcije i organiziranog kriminaliteta, Official Gazette no. 76/09, 116/10, 145/10, 57/11, 136/12, 148/13 and 70/17.

[9] Upon seizing an object, it shall be noted in the minutes where the object in question was found, the object shall be described and, where necessary, the establishment of its identity shall also be ensured in some other way. A receipt shall be issued for temporarily seized objects.

Details together with relevant case law are presented further below, and they are ordered according to different scenarios, i.e., where mobile phone was seized, and where it was not seized.

Mobile device not seized

a. Special evidentiary actions temporarily restricting certain constitutional rights of citizens (i.e., surveillance and technical recording of telephone conversations and other remote communications; interception, collection, and recording of computer data - Article 332 of the CPA

(1) Where the inquiries into criminal offences cannot be carried out in any other way or where this would entail disproportionate difficulty, the judge of investigation may, upon a written reasoned motion of the State Attorney, issue against the person suspected of having committed the criminal offence referred to in Article 334 of the present Act[10] alone or of having participated together with other persons in its

[10] 1) War crime (Article 91, paragraph 2), terrorism (Article 97, paragraphs 1, 2 and 3), financing of terrorism (Article 98), training for terrorism (Article 101), terrorist association (Article 102), slavery (Article 105), trafficking in human beings (Article 106), trafficking in human body parts and human embryos (Article 107), unlawful deprivation of liberty (Article 136, paragraph 4), kidnapping (Article 137, paragraph 3), sexual abuse of a child under the age of fifteen (Article 158), child pandering (Article 162, paragraphs 1 and 3), exploitation of children for pornography (Article 163, paragraphs 2 and 3), serious criminal offences of child sexual abuse and exploitation (Article 166), money laundering (Article 265, paragraph 4), abuse of position and authority (Article 291, paragraph 2) if the offence was committed by an official person, taking a bribe (Article 293) if the offence was committed by an official person, trading in influence (Article 295) if the offence was committed by an official person, criminal association (Article 328), committing a criminal offence as a member of a criminal association (Article 329, paragraph 1, items 3 through 6), murder of an internationally protected person (Article 352), kidnapping of an internationally protected person (Article 353), criminal offences against the Republic of Croatia (Title XXXII) and against the Armed Forces of the Republic of Croatia (Title XXXIV) punishable by imprisonment for a term of at least five years and for all criminal offences punishable by long-term imprisonment; 2) genocide (Article 88, paragraph 3), crime of aggression (Article 89, paragraphs 2 and 3), command responsibility (Article 96), recruitment for terrorism (Article 100), travelling fo the purpose of terrorism (Article 101.a), preparing criminal offences against values protected under international law (Article 103), torture and other cruel, inhuman or degrading treatment or punishment (Article 104) if committed against a child, murder (Article 110), unlawful deprivation of liberty (Article 136, paragraph 3), kidnapping (Article 137), prostitution (Article 157, paragraph 2), sexual abuse of a child over the age of fifteen (Article 159), child enticement for the purpose of satisfying sexual needs (Article 161), child pandering (Article 162), exploitation of children for pornography (Article 163), exploitation of children for pornographic performances (Article 164), abduction of a child (Article 174, paragraph 3), unauthorised manufacture of and traffic in illicit drugs (Article 190, paragraphs 2, 3 and 4), serious criminal offences against general safety (Article 222), attack on an aircraft, vessel or immovable platform (Article 223), robbery (Article 230, paragraph 2), extortion (Article 243, paragraphs 4, 5 and 6), receiving bribes in business dealings (Article 252), misuse of public procurement procedures (Article 254), avoidance of customs controls (Article 257), subsidy fraud (Article 258), money laundering (Article 265), counterfeiting money (Article 274), abuse of position and authority (Article 291),

commission a written reasoned warrant for the taking of special evidentiary actions temporarily restricting certain constitutional rights of citizens, namely:

1) the surveillance and technical recording of telephone conversations and other remote communications;
2) the interception, collection, and recording of computer data
3) entry into premises for the purpose of surveillance and the technical recording of the premises;
4) covert tailing and technical recording of persons and objects;
5) the use of undercover investigators and confidants;
6) simulated selling and purchasing of objects, simulated bribe-giving and simulated bribe-taking;
7) the provision of simulated business services or the conclusion of simulated legal transactions;
8) supervised transport and delivery of the objects of a criminal offence.

(2) By way of exception, where there is a risk of delay and the State Attorney has reason to believe that he or she will not be able to obtain the warrant of the judge of investigation in time, the warrant referred to in paragraph 1 of this Article may be issued by the State Attorney for a period of twenty-four hours. (3) The State Attorney may not issue the warrant referred to in paragraph 2 of this Article for special evidentiary actions referred to in: – paragraph 1, item 2) of this Article, if the manner in which the said action is to be taken requires entry into the suspect's home or remote entry into the suspect's computer located in the suspect's home; – paragraph 1, item 3) of this Article, if for surveillance and technical recording purposes it is necessary to enter a person's home. (4) Within eight hours from the issuance of the said order, the State Attorney shall deliver to the judge of investigation the warrant stating the time of its issuance and an official letter presenting the reasons for the warrant's issuance. In addition thereto, where he or she deems that the taking of the special evidentiary action should be continued, the State Attorney shall submit to the judge of investigation a written reasoned motion requesting that the said action be continued. Immediately upon receipt of the said warrant and official letter, the judge of investigation shall examine whether the

---

unlawful favouritism (Article 292), taking a bribe (Article 293), giving a bribe (Article 294, paragraph 1), trading in influence (Article 295), illegal entry into, movement and residence within the Republic of Croatia (Article 326, paragraph 2) and committing a criminal offence as a member of a criminal association (Article 329); 3) public incitement to terrorism (Article 99), unlawful deprivation of liberty (Article 136), rape (Article 153), serious criminal offences against sexual freedom (Article 154), prostitution (Article 157), abduction of a child (Article 174), neglect and abuse of the rights of a child (Article 177), unauthorised manufacture of and traffic in illicit drugs (Article 190), enabling the use of illicit drugs (Article 191, paragraphs 2 and 3), unauthorised manufacture of and traffic in substances banned in sports (Article 191a), extortion (Article 243), receiving or giving bribes during bankruptcy proceedings (Article 251), giving bribes in business dealings (Article 253), producing, procuring, possessing, selling or giving to another for use forgery tools (Article 283), giving a bribe (Article 294), giving a bribe for trading in influence (Article 296), disclosure of official secret (Article 300) if the offence represents a violation of the secrecy of the inquiry and fact-finding activity, giving false testimony (Article 305), preventing the presentation of evidence (Article 306), violation of secrecy of proceedings (Article 307) if the offence represents a violation of secrecy in criminal proceedings, disclosing the identity of a person in danger or protected witness (Article 308), coercion against a judicial official (Article 312), illegal entry into, movement and residence within the Republic of Croatia (Article 326), unlawful possession, making and procurement of weapons and explosive substances (Article 331), murder of an internationally protected person (Article 352), kidnapping of an internationally protected person (Article 353), attack on an internationally protected person (Article 354), threat to an internationally protected person (Article 355) and for criminal offences against computer systems, programmes and data (Title XXV) and against intellectual property (Title XXVII) if committed by the use of computer systems or computer networks.

conditions for the issuance of the warrant were fulfilled and whether the risk of delay referred to in paragraph 2 of this Article existed. (5) The judge of investigation shall issue an order deciding on the legality of the State Attorney's warrant. If the judge of investigation approves the State Attorney's warrant and the State Attorney filed a motion requesting that the evidentiary action in question be continued, the judge of investigation shall proceed as provided for in paragraph 1 of this Article. If the judge of investigation disagrees with the State Attorney's warrant, he or she shall request that the decision thereon be taken by the panel. If the taking of an evidentiary action ordered pursuant to paragraph 2 of this Article was requested to continue, the said evidentiary action shall be continued until the panel reaches its decision. The panel shall decide on the request of the judge of investigation within twelve hours from receipt of request. If the panel confirms the State Attorney's warrant and the State Attorney filed a motion requesting that the evidentiary action in question be continued, the panel shall issue the warrant referred to in paragraph 1 of this Article. If the panel does not approve the warrant, it shall issue an order requesting that the actions taken be immediately stopped, while the data collected pursuant to the State Attorney's order shall be handed over to the judge of investigation who shall destroy them. The judge of investigation shall draw up minutes of the destruction of data. (…). (7) The actions referred to in item 1 of paragraph 1 of this Article may also be ordered with respect to persons suspected of transmitting to or from the perpetrator of any of the criminal offences referred to in Article 334 of the present Act any information or messages relating to the offence, or persons whose telephone connection or any other telecommunications device the perpetrator is suspected of using, or persons suspected of hiding the perpetrator of a criminal offence or of assisting him by concealing the means by which the criminal offence was committed, the traces of the criminal offences or the objects resulting from or acquired through the commission of the criminal offence or otherwise assisting him in order to prevent his or her discovery. (8) Under the conditions referred to in paragraph 1 of this Article, the actions referred to in paragraph 1, items 1, 2, 3, 4, 6, 7 and 8 of this Article may subject to the person's written consent be taken with respect to the said person's means, premises and objects.

Use of obtained recordings, documents and objects as evidence; use of accidental finding as evidence; unlawful evidence (Article 333/1, 335/6, 338/1; 335/7)

Article 333 (1): Recordings, documents and objects obtained by the taking of actions referred to in Article 332, paragraph 1, items 1 through 8, of this Act may be used as evidence in criminal proceedings.

Article 335(6): If in the course of taking actions referred to in Article 332, paragraph 1, of this Act data and information pointing to another criminal offence and perpetrator referred to in Article 334 of this Act are recorded, this part of the recording shall be transcribed and delivered to the State Attorney and may be used as evidence in proceedings for that criminal offence.

Article 338 (1): The recordings, documents and objects obtained through the actions referred to in Article 332, paragraph 1, of this Act may be used in evidence only in proceedings against the person referred to in Article 332, paragraph 1, of this Act or in the case referred to in Article 335, paragraph 6, of this Act.

Article 335 (7): If the actions referred to in Article 332 of this Act are taken in violation of the provisions of Article 332 of this Act, the evidence learned from the data thus collected may not be used as evidence in proceedings.

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

Content of warrant (Article 335/1)

The warrant referred to in Article 332, paragraph 1, of this Act shall state the available data on the person against whom special evidentiary actions are to be taken, the facts calling for the taking of these actions and the time limit that must be appropriate for achieving the goal, as well as the manner, scope and place of taking the action. Actions shall be executed by the police. The official and responsible persons taking part in the decision-making process and the execution of actions referred to in Article 332 of this Act shall keep secret all the data that came to their knowledge in connection with the actions.

Technical assistance to police: duty and fine (Article 335/2)

The operative and technical centre for telecommunications supervision, which is responsible for ensuring technical coordination with the providers of telecommunication services in the Republic of Croatia, and the providers of telecommunication services shall provide the necessary technical assistance to the police. Where this obligation is not complied with, the judge of investigation shall, upon the motion of the State Attorney which includes a statement of reasons, fine the provider of telecommunication services in an amount not exceeding HRK 1,000,000.00 and the responsible person with the operative and technical centre for telecommunications supervision which ensures technical coordination and with the provider of telecommunication services in the Republic of Croatia in an amount not exceeding HRK 50,000.00. Where the responsible person persists in not complying with the order, he may be committed to prison until the order is executed but not for a period longer than one month. The appeal against the order imposing a fine or imprisonment shall be decided by the panel. An appeal against the order imposing a fine or imprisonment shall not stay the execution of the order.

Duration, destruction of data and information (Article 335/3-4)

(3) The special evidentiary actions referred to in Article 334 of the present Act shall be ordered for a period of up to three months. Upon the motion of the State Attorney, the judge of investigation may extend the taking of the said actions by another three months provided the actions have produced results and there is reason to continue with their taking for the purpose of collecting evidence. In the case of criminal offences referred to in Article 334, items 1 and 2, of the present Act, the taking of the said actions may, after the expiry of six months, be extended by another six months. Exceptionally, in the case of criminal offences referred to in Article 334, item 1, of the present Act, the taking of the said actions may be extended again by a further six months where this is necessary for achieving the purpose for which they were approved. The State Attorney may file within eight hours an appeal against the order of the judge of investigation rejecting the State Attorney's motion for an extension of an action, which appeal shall be decided by the panel of the same court within twelve hours. (4) As soon as the conditions referred to in Article 332, paragraph 1, of this Act cease to exist, the judge of investigation shall order that the actions taken be stopped. If the State Attorney desists from criminal prosecution or if the data and information obtained during the taking of actions are not relevant to criminal proceedings, the data and information shall be destroyed under the supervision of the judge of investigation who shall draw up a separate protocol thereof.

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

Daily reports and transcripts; final special report (Article 337/1-2)

(1) Special evidentiary actions are executed by the police, which prepares daily reports and technical transcripts on the course of their execution, which it delivers to the State Attorney on his request. At any moment during the taking of the special evidentiary actions the judge of investigation may request from the State Attorney to deliver to him a report on the course of the said actions and the need for their further taking. During the taking of special evidentiary actions the judge of investigation may, where necessary, request from the police to have daily reports and technical transcripts delivered to him for the purpose of assessing the well-foundedness of their further taking, within the scope and to the extent which he himself determines. If the actions were extended by six months (pursuant to Article 335, paragraph 3), after three months the judge of investigation must request from the State Attorney to deliver to him the report on the need for their further taking. (2) Upon expiry of the period for which the said actions were approved, the police shall draw up a special report for the State Attorney's Office and the judge of investigation in which it shall specify: 1. the dates and times the action in question started and ended; 2. the number and identity of persons with respect to whom the action in question was taken.

Time of serving the warrant (Article 335/5)

The warrant referred to in paragraph 1 of this Article shall be kept in a separate envelope. Upon completion of the action or even before its completion, where this is of benefit to proceedings, the warrant may be served on the person against whom the action was ordered if this person so requests.

Singling out recordings/transcripts/documentation for relevance (Article 338/2-3)

(2) Recordings, transcripts and documentation shall be kept sealed in the State Attorney's Office in their entirety. Where circumstances allow, the judge of investigation shall order, upon the motion of the State Attorney, that only those parts of a recording, transcript and documentation which refer to the criminal proceeding in question be included in the case file. (3) For this purpose the State Attorney shall serve on the judge of investigation a motion which includes a statement of reasons and the full version of the recording, which the judge of investigation shall return after the part of the recording which refers to the criminal proceedings in question is singled out. The singling out shall be made by an expert assistant under the supervision of the judge of investigation.

Defendant's right to have recording reproduced or transcript/documents inspected; defendant's equivalent rights at trial (Article 338/4)

The State Attorney shall enable the defendant immediately upon his request to reproduce a recording or inspect a transcript or documents. After the recording has been reproduced or the transcript or documents inspected, the defendant may propose at the trial that the recording, transcript or documents be reproduced or read out in full or in part.

Ordinance on the manner of conduct of special evidentiary actions

The sub-legal act passed in relation to the manner of conduct of special evidentiary actions is the Ordinance on the manner of conduct of special evidentiary actions[11].

a) Monitoring and technical recording of telephone conversations and other remote communications

Article 2: Surveillance and technical recording of telephone conversations and other remote communications is performed in the police premises.

Article 3: Operational-Technical Centre for Telecommunications Surveillance provides the police with technical conditions for conducting surveillance and technical recording of telephone conversations and other remote communications by capturing and transferring raw content and data from telecommunications service providers for supervised communication to the police premises.

Article 4: The police shall appropriately conduct the temporary electronic recording (storage) of the content and data of the monitored communication during the special evidentiary action referred to in Article 2 of this Ordinance at its premises and provide technical and program prerequisites for the: processing of the temporarily stored record, the recording and the delivery of recording and technical record documentation.

Article 5: With the help of appropriate technical interfaces, the police shall monitor realized telephone conversations and other remote communications and compile summaries of monitored communications, which represent the technical record documentation.

b) Interception, collection and recording of computer data

Article 6: Interception, collection and recording of computer data is carried out covertly from the police premises, and other appropriate premises.

Article 7: Interception of computer data is carried out using appropriate software solutions and technical interfaces.

Article 8: The police shall conveniently conduct temporary electronic recording (storage) of intercepted and collected data during the special evidentiary action referred to in Article 6 of this Ordinance at its premises and provide technical and program prerequisites for the: processing of the temporarily stored data, the recording and the delivery of the recording and technical record documentation.

Article 9: With the help of appropriate technical and software solutions, the police shall inspect the content of intercepted and collected computer data and compile summaries of content, which represent the technical record documentation.

(…)

Article 35

[11] Official Gazette no. 102/09. Title in original language: Pravilnik o načinu provođenja posebnih dokaznih radnji.

Daily reports and technical record documentation on the course of conducting special evidentiary actions shall be submitted by the police to the State Attorney at his or her request.
Upon completion of the ordered special evidentiary actions referred to in Articles 2, 6, 10, 16 and 31 of this Ordinance, all recordings of realized communication, intercepted and collected computer data, technical recordings of surveillance and of technical recording of premises, technical recordings of secret surveillance and of technical recording of persons and objects, as well as technical recordings of controlled transport and delivery of criminal objects, shall be recorded and delivered to the State Attorney on an appropriate electronic medium for the total duration together with the technical record documentation.

Article 36: During the implementation of special evidentiary actions referred to in Articles 2, 6, 10, 16 and 31 of this Ordinance, the police shall perform criminal-analytical processing of the collected and temporarily stored content by means of appropriate software solutions.

b. Rules relating to obtaining non-content communications data from the operator

- Checking Establishment of Contact by Means of Telecommunication for a registered owner/user - Article 339a of the CPA (formal measure, information obtained may in principle be used as evidence before court – Article 339a/9)

(1) Where there is a suspicion that a registered owner or user of a means of telecommunication committed a criminal offence referred to in Article 334 of this Act[12] or some other criminal offence punishable by

[12] 1) War crime (Article 91, paragraph 2), terrorism (Article 97, paragraphs 1, 2 and 3), financing of terrorism (Article 98), training for terrorism (Article 101), terrorist association (Article 102), slavery (Article 105), trafficking in human beings (Article 106), trafficking in human body parts and human embryos (Article 107), unlawful deprivation of liberty (Article 136, paragraph 4), kidnapping (Article 137, paragraph 3), sexual abuse of a child under the age of fifteen (Article 158), child pandering (Article 162, paragraphs 1 and 3), exploitation of children for pornography (Article 163, paragraphs 2 and 3), serious criminal offences of child sexual abuse and exploitation (Article 166), money laundering (Article 265, paragraph 4), abuse of position and authority (Article 291, paragraph 2) if the offence was committed by an official person, taking a bribe (Article 293) if the offence was committed by an official person, trading in influence (Article 295) if the offence was committed by an official person, criminal association (Article 328), committing a criminal offence as a member of a criminal association (Article 329, paragraph 1, items 3 through 6), murder of an internationally protected person (Article 352), kidnapping of an internationally protected person (Article 353), criminal offences against the Republic of Croatia (Title XXXII) and against the Armed Forces of the Republic of Croatia (Title XXXIV) punishable by imprisonment for a term of at least five years and for all criminal offences punishable by long-term imprisonment; 2) genocide (Article 88, paragraph 3), crime of aggression (Article 89, paragraphs 2 and 3), command responsibility (Article 96), recruitment for terrorism (Article 100), travelling fo the purpose of terrorism (Article 101.a), preparing criminal offences against values protected under international law (Article 103), torture and other cruel, inhuman or degrading treatment or punishment (Article 104) if committed against a child, murder (Article 110), unlawful deprivation of liberty (Article

imprisonment for a term of more than five years the police may, on the basis of a warrant issued by the judge of investigation and for the purpose of collecting evidence, *via the Operational-Technical Centre for Telecommunications Surveillance* request from the provider of publicly available communications services to check the identity, duration and frequency of communication with particular electronic communication addresses, to determine the location of a communications device and the location of persons establishing electronic communications and to identify the device.

(2) For the registered owner or user of a means of telecommunication that is connected with the person suspected of having committed a criminal offence referred to in Article 334 of this Act or some other criminal offence punishable by imprisonment for a term of more than five years the police may, on the basis of a warrant issued by the judge of investigation, *via the Operational-Technical Centre for Telecommunications Surveillance* request from the provider of publicly available communications services to perform the check referred to in paragraph 1 of this Article.

136, paragraph 3), kidnapping (Article 137), prostitution (Article 157, paragraph 2), sexual abuse of a child over the age of fifteen (Article 159), child enticement for the purpose of satisfying sexual needs (Article 161), child pandering (Article 162), exploitation of children for pornography (Article 163), exploitation of children for pornographic performances (Article 164), abduction of a child (Article 174, paragraph 3), unauthorised manufacture of and traffic in illicit drugs (Article 190, paragraphs 2, 3 and 4), serious criminal offences against general safety (Article 222), attack on an aircraft, vessel or immovable platform (Article 223), robbery (Article 230, paragraph 2), extortion (Article 243, paragraphs 4, 5 and 6), receiving bribes in business dealings (Article 252), misuse of public procurement procedures (Article 254), avoidance of customs controls (Article 257), subsidy fraud (Article 258), money laundering (Article 265), counterfeiting money (Article 274), abuse of position and authority (Article 291), unlawful favouritism (Article 292), taking a bribe (Article 293), giving a bribe (Article 294, paragraph 1), trading in influence (Article 295), illegal entry into, movement and residence within the Republic of Croatia (Article 326, paragraph 2) and committing a criminal offence as a member of a criminal association (Article 329); 3) public incitement to terrorism (Article 99), unlawful deprivation of liberty (Article 136), rape (Article 153), serious criminal offences against sexual freedom (Article 154), prostitution (Article 157), abduction of a child (Article 174), neglect and abuse of the rights of a child (Article 177), unauthorised manufacture of and traffic in illicit drugs (Article 190), enabling the use of illicit drugs (Article 191, paragraphs 2 and 3), unauthorised manufacture of and traffic in substances banned in sports (Article 191a), extortion (Article 243), receiving or giving bribes during bankruptcy proceedings (Article 251), giving bribes in business dealings (Article 253), producing, procuring, possessing, selling or giving to another for use forgery tools (Article 283), giving a bribe (Article 294), giving a bribe for trading in influence (Article 296), disclosure of official secret (Article 300) if the offence represents a violation of the secrecy of the inquiry and fact-finding activity, giving false testimony (Article 305), preventing the presentation of evidence (Article 306), violation of secrecy of proceedings (Article 307) if the offence represents a violation of secrecy in criminal proceedings, disclosing the identity of a person in danger or protected witness (Article 308), coercion against a judicial official (Article 312), illegal entry into, movement and residence within the Republic of Croatia (Article 326), unlawful possession, making and procurement of weapons and explosive substances (Article 331), murder of an internationally protected person (Article 352), kidnapping of an internationally protected person (Article 353), attack on an internationally protected person (Article 354), threat to an internationally protected person (Article 355) and for criminal offences against computer systems, programmes and data (Title XXV) and against intellectual property (Title XXVII) if committed by the use of computer systems or computer networks.

(3) The judge of investigation shall decide on the State Attorney's request within four hours. The judge of investigation shall issue the warrant for the performance of the check referred to in paragraphs 1 and 2 of this Article on the basis of a reasoned motion of the competent State Attorney.

(4) By way of exception, if there is a risk of delay and if the State Attorney has reason to believe that he or she will not be able to obtain the warrant of the judge in time, the warrant referred to in paragraphs 1 and 2 of this Article may be issued by the competent State Attorney.

(5) The warrant referred to in paragraph 4 of this Article and the official letter explaining the reasons for the warrant's issuance shall be delivered by the State Attorney to the judge of investigation immediately and no later than twenty-hour hours from its issuance.

(6) The judge of investigation shall issue the order deciding on the legality of the State Attorney's warrant within forty-eight hours from receipt of the warrant and the official letter. Against the order of the judge of investigation the State Attorney shall have no right of appeal.

(7) In addition to the information referred to in Article 168, paragraph 2, of the present Act[13], the warrant referred to in paragraphs 1, 2 and 4 of this Article shall include the personal data of the person that is the registered owner or user of the means of communication in question and the purpose for which the warrant has been issued.

(8) The warrant for checking the establishment of contact by means of telecommunication is not necessary if the registered owner or user of the means of communication has given his written consent.

(9) If the information referred to in paragraphs 1 and 2 of this Article was obtained without the warrant of the judge of investigation or if the State Attorney failed to deliver the warrant to the judge of investigation within the period referred to in paragraph 5 of this Article or if the State Attorney's request for the authorisation of the warrant for checking the establishment of contact by means of telecommunication has been refused, the information thus obtained cannot be used in evidence in the proceedings.

- Police authority to verify contact by electronic communications: Article 68 of the Police Duties and Powers Act (PDPA), in connection with Article 207 of the CPA on inquiries into criminal offenses (below)

Verification of contact by electronic communications represents one of the police powers under the Police Duties and Powers Act[14] (Article 13, paragraph 1, item 13).[15]

[13] Contents of the warrant: 1) Name of the authority; 2) the full name and function of the official person or persons who issued the order or warrant/injunction; 3) the full name of the recorder if the decision was taken during a session; 4) the full name of the defendant and his or her citizen's identification number; 5) the criminal offence tried; 6) the date of issue of the order or warrant/injunction (Article 168, paragraph 2 of the CPA).
[14] Zakon o policijskim poslovima i ovlastima , Official Gazette no. 76/09, 92/14 and 70/19.

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

Article 68 (PDPA)

1) In order to prevent and detect criminal offenses prosecuted ex officio and their perpetrators, to prevent danger and violence, to search for persons and objects, the police may request the communication service provider to verify the identity, duration and frequency of communication with certain electronic communication addresses. (2) The request referred to in paragraph 1 of this Article may also include determining the position of the communication device, as well as determining the location of persons establishing electronic communication and the identification marks of the device. (3) The request referred to in paragraph 1 of this Article shall be based on the written approval of the Chief of the Criminal Police Directorate, or the Chief of the National Police Office for the Suppression of Corruption and Organized Crime or the Chief of the Police Administration, and in their absence persons replacing them. (4) As an exception to paragraph 3 of this Article, if this is necessary to prevent imminent danger or violence or to search for persons urgently, the approval may be given orally, but must be confirmed in writing no later than 24 hours from the given oral approval. (5) The approval referred to in paragraphs 3 and 4 of this Article shall be based on the facts from which it is evident that other actions could not or will not be able to achieve the goal of police work or that
the achievement of that goal would involve disproportionate difficulties.

Operators' duty to dispatch to the police call records in response to claims on alleged nuisance or malicious calls and SMS/MMS messages under the Law on Electronic Communications

The Law on Electronic Communications[16] prescribes in Article 105 a specific procedure for handling alleged nuisance or malicious calls and SMS/MMS messages, which interferes with prescribed confidentiality of communications. According to this Article any false representation of callers or senders of SMS messages and MMS messages is prohibited in public communications networks. Exclusively on the basis of subscriber's/user's written request indicating their receiving of nuisance/malicious calls or messages, the operators are obliged to determine identity (name and surname or company name) and address of the end-user from whom those calls or messages originated. They also must retain the data, which include identification details of the caller or sender of SMS/MMS messages and the date and time

[15] Note: section 13 of the Code of Practice of Police Officers contains details on police activity of verification of the establishment of electronic communication.Verification of the establishment of electronic communication is carried out through the application of a computer system for managing the requirements for verification of the establishment of electronic communication. The persons authorized to submit the Request for verification of the establishment of electronic communication are: - police officer for crime processing, - Chief of the Operational-Communication Center of the Police, - shift manager of the Police Operational-Communication Center, - Assistant Shift Manager of the Police Operational Communication Center. The request is approved by the authorized signatory on the basis of the prior consent of the authorized managers, as follows: - Head of the Sector in the Criminal Police Directorate, - Head of the Service in the Criminal Police Directorate, - Head of the Sector / Head of the Criminal Police Service in the Police Administration, - Head of the Service / Department / Section in the Criminal Police of the Police Administration, - Chief of Police Station.

[16] Title in original language: Zakon o elektroničkim komunikacijama (Official Gazette no. 73/08, 90/11, 133/12, 80/13, 71/14 and 72/17).

thereof. Following this they are obliged to immediately dispatch the data to competent police authorities for further procedure in accordance with the special law, of which they must inform the subscriber/user who filed the request in writing.

Pre-trial phases enabling data collection uner the CPA: inquiries, urgent evidentiary actions, evidentiary actions when the perpetrator is unknown

- Inquires into Criminal Offences – Article 207 of the CPA

(1) If there are grounds for suspicion that a criminal offence prosecuted ex officio was committed, the police have the right and the duty to take the necessary measures to: 1) find the perpetrator of the criminal offence, to prevent the perpetrator of or the participant in a criminal offence from going into hiding or fleeing; 2) discover and secure the traces of a criminal offence and objects that may be used for establishing the facts; and 3) collect all information that might be useful for the successful conduct of criminal proceedings. (2) The police shall inform the state attorney in due time of the inquiries undertaken into criminal offences. If the State Attorney informs the police of his or her intention to be present at the conduct of particular inquiries or the taking of particular measures, the police shall conduct the inquiries or take the measures in a way that allows for such State Attorney's presence. (3) On the facts and circumstances established during the taking of the actions referred to in paragraphs 1 and 2 of this Article, which facts and circumstances might be of interest for the criminal proceedings, the police shall draw up an official note.
(4) On the basis of the conducted inquiries the police shall prepare in accordance with a special act the crime report or the report on the conducted inquiries in which it shall state the evidence it found. The crime report or the report shall not include the contents of the statements given by particular citizens in the course of the gathering of information. The crime report or the report shall be accompanied by objects, sketches, pictures, files on the measures and actions taken, official notes, statements and any other material that might be of use for the successful conduct of proceedings. (5) If the police subsequently learns of new facts or evidence or detects any traces of a criminal offence, it shall collect all necessary information and in due time deliver the report thereon to the State Attorney.
(6) When conducting inquiries into criminal offences the police shall proceed in accordance with both the provisions of a special act[17] and the rules adopted pursuant to such act.

- Urgent Evidentiary Actions - Article 212 of the CPA

(1) Where there is a risk of delay, the police may, even before the institution of criminal proceedings for criminal offences punishable by imprisonment for a term of up to five years, conduct searches (Article 246), temporarily seize items (Article 261), conduct identification (Article 301), conduct inspections (Article 304) and take fingerprints and prints of other body parts (Articles 211 and 307). (2) In the case of criminal offences punishable by imprisonment for a term of over five years, the police shall inform immediately the state attorney of any risk of delay or the need to collect evidence, except where the acts of collection of evidence concern temporary seizure of items (Article 261) or searches (Article 246). The

[17] Such as the PDPA.

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

state attorney may perform the evidence-collecting acts referred to in paragraph 1 of this Article himself/herself or may leave it to the police or order the investigator to perform them. A state attorney who arrives at a location where an inspection or a search is underway may take over the performance of the act. (3) Where the acts referred to in paragraphs 1 and 2 of this Article need to be performed in respect of an official person who is authorised and duty bound to detect and report criminal offences prosecuted ex officio, the police shall immediately inform thereof the state attorney who shall decide whether he/she himself/herself will perform those acts or whether he/she will order the investigator to perform them. (4) Where there is a risk of delay, the state attorney may request the necessary expert examinations to be performed**,** except exhumation. (5) The police shall inform the state attorney without delay of the results of acts performed by it under paragraphs 1 and 2 of this Article.

- Evidentiary Actions When the Perpetrator is Unknown – Article 214 of the CPA

(1) If the perpetrator of a criminal offence is unknown, the State Attorney may take or order to the investigator the taking of evidentiary actions if this is expedient for detecting the perpetrator or if there is a risk of delay.
(2) The police may, if that is expedient to identify the perpetrator, order the necessary expertise (….)
(3) Of all that has been done the police or the investigator shall inform the State Attorney prior to or, where this is not possible, immediately after the taking of an action.

Legality of evidence

Examples of ex lege unlawful evidence, i.e., evidence obtained in violation of criminal procedure rules that are as such (having as a consequence illegality of evidence obtained) expressly provided by the CPA (Article 10, paragraph 2, item 3 of the CPA)

a. violation of Article 332 of the CPA
   if the actions referred to in Article 332 of this Act are taken in violation of the provisions of Article 332 of this Act, the evidence learned from the data thus collected may not be used as evidence in proceedings (335/ 7)

b. violation of Article 339a of the CPA
   Article 339a/ 9: If the information was obtained without the warrant of the judge of investigation or if the State Attorney failed to deliver the warrant to the judge of investigation within the prescribed period (referred to in paragraph 5) or if the State Attorney's request for the authorisation of the warrant for checking the establishment of contact by means of telecommunication has been refused, the information thus obtained cannot be used in evidence in the proceedings.

Case law (mobile phone not seized)

- Unreasoned/inadequate reasoning of the warrant - secret telecommunication surveillance (Article 332 of the CPA) [18]
- Photographing mobile phone and data in mobile phone of a witness

Mobile device of a witness had not been seized by the police and no search of a mobile phone was conducted. The police photographed the phone as well as the data contained in it (specifically photographs made in a public space). All this was voluntarily provided and made available to the police by the witness - owner of device. The Supreme Court rejected the defendant's appeal and affirmed the decision of the court of first instance rejecting the claim for exclusion of such evidence (photographs) as unlawful under Article 10 (paragraph 2, item 3)[19] of the CPA. While the Court did not expressly note that there was a violation of Article 263 of the CPA on temporary seizure of „data saved in computers and devices connected thereto, as well as in devices used for collecting and transferring data, to data carriers and to subscription information in the possession of a service provider", in justifying its decision it did note also that „Article 263 of the CPA does not expressly mention the data contained in the mobile phone and that no provision of the CPA forbids the use of data obtained in contravention of Article 263 as evidence in the proceedings.[20] Comment: Article 263 in my opinion does relate also to the data in the mobile phone, however, there is a scarcity of (final) decisions referring to and interpreting Article 263 of the CPA in connection with Article 261 of the CPA in the used case-law databases.[21]

In another case the Supreme Court affirmed the decison of the court of first instance allowing as evidence the photography of the accused in form of a contact in the mobile phone of the witness, made by police officers, and the corresponding CD. According to the Court, the warrant of the judge of investigation was not necessary for such action of the police, since the witness on her own and voluntarily read out the contents of her mobile phone on the contact with the accused and voluntarily handed her mobile phone to the police officers so that they could make a photography of that contact. [22]

Where the police photographed mobile phones of witnesses, including a photography of a message on Facebook profile on the mobile phone of a witness, and the defendants claimed that such evidence (photo-documentation of the inspection: photography of the mobile phone of the witness and photography of a message on their Facebook profile) was unlawful, the courts, when denying such claims, must provide adequate argumentation for reaching their decision that the evidence is lawful and it is not enough to only state that the mobile phones in question were handed to the police voluntarily. The reasons for their decision and the way that the police obtained the mobile phones in question must be evident from court files and it must be established during trial (e.g. in questioning before the judge) if the mobile phones had

[18] ECHR case law: Dragojević v. Croatia, no. 68955/1; Bašić v. Croatia, no. 22251/13, Matanović v Croatia, no. 2742/12; Grba v. Croatia, no. 47074/12, Parazajder v. Croatia, no. 50049/12; Bosak and others v. Croatia, nos. 40429/14 and 3 others. Also see judgments of the Supreme Court of Republic of Croatia: I Kž-Us 7/2018-6, 13.2.2020.; I Kž-Us 165/2017.-4., 08.2.2018; I Kž-Us 26/17.-5, 04.5.2017; I Kž-Us 26/17.-5, 05.9.2017. For decisions of the Constitutional Court, see: U-III-1360/2014, 10.12.2019.

[19] Evidence was not "obtained in violation of criminal procedure provisions which is expressly provided for in the Criminal Procedure Act".

[20] Supreme Court of the Republic of Croatia, decision, I Kž 669/2018-4, 05.12.2018.

[21] E.g. Supreme Court of Republic of Croatia, I Kž-Us 3/17.-4.

[22] Supreme Court of the Republic of Croatia, decision, I Kž-Us 28/2020-4, 09.4.2020.

been provided to the police voluntarily, if their owners unlocked them and thus enabled a search of their content (charge: murder). In the present case, therefore, the Supreme Court accepted the defendant's appeal to the lower court's decision refusing to exclude from court file as unlawful mentioned evidence thus obtained.[23]

Where it is not enough documented how the photographs of SMS messages were obtained by the police (in concrete case content of SMS both of the defendant and the injured party), i.e., it was only stated that the photo-documentation is classified as „inspection", the courts must, where they base their decisions also on such photographs justify their decision denying defendant's claim on unlawful evidence and exclusion from court file, whether during the trial upon defendant's claim on exclusion of such evidence or at the latest in the judgment. The right of a defendant to a reasoned court decision was breached. In the case at hand the Supreme Court as appelate court accepted the defendant's appeal, remanded the case to the court of first instance for retrial and instructed the court of first instance to provide adequate reasons. [24]

Defendant claimed illegality of evidence in form of a photographed mobile phone of the injured (aggrieved) party and SMS messages contained in it (allegedly provided voluntarily by the injured party to the police officers, not in context of a search). The first-instance court did not during the proceedings provide reasons for rejecting the defendant's motion on exclusion of such evidence as unlawful. It also did not state in the impugned verdict that the defendant proposed the exclusion of such evidence as illegal evidence, nor did it provide reasons for rejecting such a motion in the verdict itself. The first-instance court only stated arbitrarily in the minutes from the hearing that this would not be illegal evidence because it was not a search of a mobile phone owned by the injured party, which that injured party voluntarily handed to police officers so that they could take photographs of SMS messages. The appellate court, therefore, remanded the case to the court of first instance for retrial. In renewed procedure the court of first instance needs to also examine whether such evidence was obtained as fruit of a poisonous tree, i.e., as a consequence of illegal search of the defendant's mobile device, because of which that court excluded from court files the records from the defendant's mobile phone and details of calls.[25]

- Call records and data from operators (Article 339a CPA/Article 68 of the PDPA)

In a number of cases the defendants claimed that the telecommunications data (evidence) obtained under Article 68 of the PDPA was unlawful (e.g. reports on insight and analysis in collections and registers of telecommunication operators), as it was not obtained with the order of judge of investigations under the rules of Article 339a of the CPA, which due to court's control preserve the constitutional right to secrecy of correspondence and other types of communication. Where the data relate to registered owner or user and criminal offense in question falls under Article 339a of the CPA and, in order for such evidence to be legal, i.e., on which a court decision may be based, the courts normally do not accept as evidence such data where it was obtained by the police in application of Article 68 of the Police Powers and Duties Act. Where such data is used as evidence in the proceedings and the court based its judgment on them, the

[23] Supreme Court of Republic of Croatia, decision, I Kž 111/16-4, 24.2.2016.
[24] Supreme Court of Republic of Croatia, I Kž 329/2017-4, decision, 24.2.2016.
[25] County Court in Pula, decision, Kž-210/2017-7, 19.12.2017.

judgment in question is normally quashed.[26] Where Article 339a of the CPA cannot apply (e.g. the offense in question is punishable by imprisonment under 5 years), the courts accepted the data obtained by the police (if formal requirements have been met under Article 68 of the PDPA) - but not as evidence on which a judgment is based but rather as a result of police inquiry measures (the result of which, e.g., could be useful to the State Attorney for the taking of further measures in the investigation or evidentiary procedure). The same applies where the telecommunications data sought relate to unregistered owner/user.[27]

- Written consent of registered device owner (Article 339a - no warrant + *any offense?*)

In another recent (ongoing) case the court of second instance confirmed the lower court's decision on rejection of defendant's motion to exclude from files as unlawful evidence, call records from his mobile phone as obtained from the telecom provider, which, according to the defendant were obtained contrary to Article 339a of the CPA. The offense at hand was not included in a catalogue of offenses for which such action could have been ordered under mentioned CPA provision and there was no warrant. However, owner of the mobile phone gave written consent to undertake such a measure (specified in Article 339a), by which under Article 339a a warrant would not be required. In that way, the court held that the defendant waived the constitutionally guaranteed right to the freedom and secrecy of correspondence. The measure (Article 339a) could according to this court, in case of written consent of a registered owner of a mobile device, essentially apply in cases of all criminal offenses. In this sense, therefore, the court confirmed that the data (evidence) thus obtained was lawful.[28]

- Fruit of the poisonous tree

Where evidence (data relating to telecom operator's files and registries for a certain mobile phone, together with a list of contents of the mobile phone) is obtained by a warrant of the judge of investigations, but which warrant was issued (as evident from reasons provided in the warrant) on the basis of evidence that was excluded from the file as unlawful („report on an overview of analytic information of telecommunications traffic list for a SIM card"), such evidence shall also be unlawful.[29] (Conversely, where reasoning of the warrant provided by the judge of investigations, in this case, for a search of a mobile phone, does not point to that judge's reliance on evidence that was excluded from court

[26] Supreme Court of Republic of Croatia, decision, I Kž 290/2017-4, 01.6.2017. For more case law, see: Supreme Court of Republic of Croatia, III Kr 28/2017-7, 11.7.2019; Supreme Court of Republic of Croatia, III Kr 31/2018-6, 25.10.2018; Supreme Court of Republic of Croatia, I Kž-Us 150/15-5, 19.1.2017.

[27] Thus, for example, according to the recent judgment of the Supreme Court, as in the specific case the police did not know who the registered owner or user of the number in question was, it lawfully used its powers under Article 68 of the Police Duties and Powers Act in the scope of police inquiry. The police report was compiled in line with Article 207 of the Criminal Procedure Act as a result of conducted police inquiries and the data and facts that were found out during the inquiries were obtained and established in a lawful manner and they have cognitive value. Mentioned report on conducted inquiries, as well as filed crime report, in relation to their content, in any case do not constitute evidence, so they cannot be excluded from the court file as unlawful evidence. Supreme Court of Republic of Croatia, judgment, Kzz 2/2020-3, 08.5.2020.

[28] County Court in Varaždin, judgment, 8 Kž-361/2019-7, 03.10.2019.

[29] Supreme Court of the Republic of Croatia, decision, I Kž 121/2019-4.

files as unlawful (as mentioned above), then evidence collected on the basis of such warrant shall not be excluded from court files as unlawful.)[30]

- Differences between Article 339a / Article 332 measures and privacy thresholds: no reasoned warrant for Art. 339a as required for Art. 332 measure

The Supreme Court denied in its practice claims that the data collected by verification of telecommunication contact (Article 339a) represented evidence obtained by infringement of right to inviolability of personal and family life guaranteed by the Constitution and international law, and/or evidence obtained in violation of criminal procedure provisions (as well as all other evidence gained from such data).
The Supreme Court acknowledges in its case law that the measure in Article 339a, i.e., obtaining the data on the identity, duration and frequency of telecommunications, position of communication devices, as well as places where persons who establish such communication, constitutes an interference with the right to respect for "private life" and "correspondence" guaranteed by Article 8 of the European Convention on Human Rights and Articles 35 and 36 of the Constitution of the Republic of Croatia. [31] However, such data in Article 339a "only concern the previously established contacts, location of communication devices and of persons at the time of establishing such contact, but not also the content of their communication. For that reason, according to the Court, the legislator prescribed lower standards for their obtaining under Article 339a than for special evidentiary actions in Article 332 of the CPA. Thus in respect to defendant's claim that the warrant for such data by judge of investigation was not reasoned, in particular on the circumstance "where the inquiries into criminal offences cannot be carried out in any other way or where this would entail disproportionate difficulty" (as prescribed in Article 332), the Court confirmed that the duty of a reasoned warrant does not fall in the scope of Article 339a, which measure is entirely different from a special evidentiary measure in Article 332 (the latter requires such reasoned warrant). While the warrant issued by the judge of investigations under Article 339a does not need to be reasoned, his/her warrant is issued on the basis of a reasoned motion of the competent State Attorney (Article 339a, paragraph 3 of the CPA). According to the Court, such duty to reason the motion for the warrant enables the judge of investigations to examine justification of that measure in advance, in order to thoroughly check (judicial scrutiny) whether the legal conditions for its application are met and whether the use of such a measure is necessary and proportionate in given circumstances. Therefore claims that the data collected by verification of telecommunication contact (Article 339a) represented evidence obtained by infringement of right to inviolability of personal and family life guaranteed by the Constitution and international law, and/or evidence obtained in violation of criminal procedure provisions, as well as all evidence gained from such unlawful evidence, were denied. [32]

Mobile device seized

[30] Supreme Court of the Republic of Croatia, decision, I Kž 121/2019-4
[31] See, e.g. Supreme Court of Croatia, decision, I Kž 150/17-4, 12.4.2017.
[32] Supreme Court of Republic of Croatia, decision, I Kž 150/17-4, 12.4.2017.

Legality of evidence

Examples of *ex lege* unlawful evidence, i.e., evidence obtained in violation of criminal procedure rules that are as such (having as a consequence illegality of evidence obtained) expressly provided by the CPA

- unlawful search as stipulated in Article 250
- temporarily seized files/ documents, recordings and notes, which cannot be seized (Article 262/7)
- finding and opinion of a person who may not be appointed as expert witness (Article 311/1[33])

Case law (mobile phone seized)

- Temporary seizure of defendant' mobile phone in his home without a search warrant (inquiries, voluntary provision)

Defendant's mobile phone, tablet and laptop were seized in his home by the police without a search warrant. The defendant therefore claimed the evidence obtained on the basis of such illegal search was illegal. However, the court found that the police seized those objects as part of their police authority under Article 207 of the CPA and that the defendant voluntarily handed over such objects, in line with his duty under Article 261, paragraph 2 of the CPA, signed the minutes on temporary seizure and provided no comments to it. Had the defendant refused to voluntarily hand over the stated objects, the police would have been obliged to obtain a warrant and conduct a search of the defendant's home.[34]

- Mobile phone seized unlawfully (no consent in circumstances of leading to unlawful evidence obtained by search of that phone (content) / also a case where procedural breach such as violation of Article 262/ 6 on minutes on seizure of a movable would not in itself amount to illegality of evidence

Minutes on search of the mobile phone represents unlawful evidence, where it became known from the unlawfully seized mobile phone, which may not be used as evidence in the proceedings. In the concrete case the mobile phone, as evidence which may be used in criminal proceedings, was seized by the police in the defendant's home without consent of the defendant, which "search" of a home was conducted without a warrant in contravention of the CPA: Such unlawfulness is not remedied by the fact that defendant as mobile phone owner was "cooperative" in the police station, after his mobile phone had already been unlawfully seized by the police, and that he himself opened the mobile phone and took out

[33] A person who may not be interrogated as a witness or who is exempt from the duty to testify or against whom the criminal offence in question was committed may not be appointed as an expert witness and if such a person is appointed, his or her findings and opinion may not be used as evidence in the proceedings.
[34] Supreme Court of the Republic of Croatia, Kžm 18/16-8, 13.10.2016.

SIM cards. Also, provisions of the Police Duties and Powers Act on police authority to temporarily seize objects (Articles 57, 59) do not regulate the way of seizing objects intending to serve as evidence in criminal proceedings.[35] On the other hand, the Court noted that the shortcoming that the minutes on seizure of a movable did not contain a note where the object was found (as prescribed by Article 262, paragraph 6 of the CPA[36]), would not by itself render such evidentiary action unlawful.[37]

- Stored data in mobile phone obtained lawfully by search, special evidentiary measures (secret surveillance) not applicable

The Supreme Court confirmed the decision of the court of first instance, which denied the defendant's request to exclude as unlawful evidence the e-mail correspondence and list of SMS messages, obtained during search of a mobile phone. According to the defendant, his rights under Article 36 of the Constitution[38] and Article 8 of the European Convention on Human Rights were violated, since such evidence should have only been obtained on the basis of Article 332 of CPA on special evidentiary measures (secret surveillance). The court confirmed that the present case did not call for special evidentiary actions such as telecommunications surveillance. As regards content of the mobile phone in which information (evidence) is stored, such evidence was lawfully obtained, since the provisions on search of a mobile phone and the data in it have been complied with. Consequently, there was also no violation of Article 36 of the Constitution and Article 8 of the European Convention on Human Rights.[39]

- Recording of data from searched computer/server (Article 257 on search – no need for secret surveillance in Article 332) to a hard drive was conducted in line with Articles 261 and 263 of the CPA (possible application per analogy to mobile phones/data)

Defendant's claim that the search of a computer and/or server was done in contravention of the CPA, Article 36 of the Constitution and Article 8 of the European Convention on Human Rights, and thus constituted illegal evidence that should be excluded from the proceedings/court files, was denied by the

[35] Supreme Court of the Republic of Croatia, decision, I Kž 658/15-4, 12.1.2016.
[36] "Upon seizing an object, it shall be noted in the minutes where the object in question was found, the object shall be described and, where necessary, the establishment of its identity shall also be ensured in some other way. A receipt shall be issued for temporarily seized objects."
[37] Supreme Court of the Republic of Croatia, decision, I Kž 658/15-4, 12.1.2016.
[38] "The freedom and privacy of correspondence and all other forms of communication shall be guaranteed and inviolable. Restrictions necessitated by the protection of national security and the conduct of criminal prosecution may be prescribed solely by law."
[39] See, e.g. Supreme Court of Republic of Croatia, I Kž-Us 103/15-4, 15.9.2015. Comment: unfortunately the lower court's decision with detailed explanation by which it denied the motion to exclude from court file such evidence as unlawful, which this court hereby confirmed, is not available in used case-law database, and the present decision of the Supreme Court does not re-examine the legal issue of search of the mobile phone and data with reference to relevant provisions of the CPA.

Court. The Court denied the claim of the defendant that special evidentiary actions (secret surveillance) should have applied in this case, since in this case there was no need for secret surveillance - the data were already stored in the computer and server, the search of which was conducted lawfully (in line with Article 257). Rules on temporary seizure of objects, which apply also to „data saved in computers and devices connected thereto, as well as in devices used for collecting and transferring data, to data carriers and to subscription information in the possession of a service provider" in Articles 261 and 263 of the CPA were also complied with during the recording of data from searched computer and server to a hard disk.[40]

- Acting contrary to Article 257 (2) of CPA by not taking measures to prevent data destruction/ modification during search does not make evidence obtained unlawful per se (possible application per analogy to mobile phone/data)

The Supreme Court affirmed the lower court's decision denying the defendant's request to exclude from files as evidence minutes on search of a movable (laptop) together with related evidence. The defendant claimed that the police did not take measures to prevent the destruction or modification of data in her computer, which was seized and searched some time after she was arrested, so that the data could have been manipulated when the computer was out of her reach (alleged contravention of Article 257, paragraph 2 of the CPA[41]). Besides such claim not being backed up by any argumentation, the Supreme Court found that such claim would not affect the legality of conducted search under Article 257 (once the laptop was temporarily seized, and searched the next day under the warrant and with presence of the defense counsel) and of evidence thus obtained (minutes of the search). Namely, acting contrary to Article 257, paragraph 2 of the CPA does not make the action or evidence obtained by the search illegal, because the same is not prescribed in Article 250 of the CPA. In order for the evidence to be illegal (in the sense of Art. 10, paragraph 2, item 3, of the CPA), it must be obtained in violation of the provisions of criminal procedure and its illegality expressly provided by law. Any defendant's claim on potential manipulation may only be examined from the point of view of reliability, which is possible in the further phase of the proceedings.[42]

- The issue if search of SD memory card for which no warrant was issued could contaminate the computer for which warrant existed, as well as the issue of "unprofessional" way of conducting a computer search is possibly an objection to

[40] Supreme Court of Republic of Croatia, I Kž-Us 3/17.-4., 26.1.2017.
[41] Upon the order of the authority carrying out a search, the person using a computer or having access to a computer and other devices referred to in paragraph 1 of this Article, and a telecommunications service provider, shall immediately take measures to prevent the destruction or modification of data. The authority carrying out a search may order that an expert assistant take these measures.
[42] Supreme Court of Republic of Croatia, Kžm 25/2019-4, decision, 05.9.2019.

credibility of evidence, i.e., minutes of computer search (possible application per analogy to mobile phones/data)

The Supreme Court denied the request of the accused person for extraordinary review of final judgment, and according to this decision, claims on lack of reliability of evidence were discussed before the first and second instance court and expert examination was conducted, during which disputable issues were clarified: "… the accused unsuccessfully complains about the legality of the search of the laptop […], stating that the laptop was not only the subject of the search but at the same time a means for the otherwise illegal search of the SD card, because the contents of that card were viewed on the laptop in question. This information, connected with an extremely unprofessional search of the laptop (which the applicant corroborates by claiming that no so-called backup was made on the computer before opening the files in the computer) resulted in the fact that during the expert examination it was no longer possible to determine whether files were opened [at a specific time period], including those that are the subject of the incrimination, which made it impossible to verify the authenticity of the testimony of witness. The accused himself added that memory cards were inspected on his laptop which were found in the bag, instead of on another computer, which enabled the transfer of files from memory cards to the computer and vice versa, which means that after that neither the computer nor memory cards could be credible evidence due to suspicion of their contamination."

The Court confirmed the findings of both the first and second instance court, that the laptop was searched on the basis of a previously issued search warrant, so the defense's motion to separate the evidence as unlawful was properly rejected: "The fact that on the same occasion, when the computer was searched, the SD memory card was searched on the same computer, for the search of which no warrant of the investigating judge was issued, so that part of the search record was separated as unlawful (by first and second instance court decisions), does not make the computer search illegal. These are two searches that each form a separate unit, and the fact that one protocol (minutes) was made of both did not result in a different qualification of these actions as separate evidence. Finally, illegality of the search of the SD memory card led to the exclusion of the part of search minutes related to search of that card. The question, however, whether and to what extent the search of the SD memory card for which no warrant was issued by the investigating judge, could "contaminate" with its content the computer for which the warrant existed, is possibly an objection to the credibility of evidence, i.e., minutes of the computer search, which is essentially a question of fact, and on what grounds the filing of this extraordinary remedy is not permitted. Of the same meaning is the "unprofessional" way of conducting a computer search, which is explained in detail by the accused, i.e., the consequent inability to determine the earlier dates of access to individual files. The first-instance and second-instance courts commented on these allegations of the accused, which actually warn of certain shortcomings and shortcomings of the probative value of conducted search, after an expert examination was conducted, during which all disputable issues were clarified, since that is also a matter of objection on credibility of evidence, and not its lawfulness."

As regards the SD card, the Court noted that although it was searched unlawfully the first time, the card was searched subsequently upon the issued warrant and thus such latter search thereof was lawful: "the fact that content of the mentioned memory card was determined for the first time on the basis of an illegal search did not result in the illegality of the holder of that content - the SD memory card itself."[43]

[43] Supreme Court of Republic of Croatia, judgment, III Kr 165/11-5, 19.9.2012.

- Generally: shortcomings / lacking in reasoning in the search warrant (issued, as such, on the basis of reasoned request in detail by the State's Attorney) would not make minutes on the search unlawful per se (not specified in Article 250 of the CPA) [44]

Personal data protection in criminal proceedings: general overview

The CPA still contains a reference to the Council Framework Decision 2008/977/JHA of 27 November 2008 on the protection of personal data processed in the framework of police and judicial cooperation in criminal matters, and no provisions were amended and/or added in order to transpose the Data Protection Law Enforcement Directive (EU) 2016/680. Instead, the legislator opted to transpose that Directive via a new act - Act on the protection of natural persons with regard to the processing and exchange of personal data for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties (Official Gazette no. 68/2018). [45] Since the act is relatively new, no records relating to this act were found in online databases used by this researcher.

Current general provisions of the CPA on the processing of personal data are Articles 186-188g (Articles 186a-188g mainly relate to the exchange/transfer of personal data):

Article 186

(1) Personal data may be collected by the competent authorities only for purposes specified by law in the framework of their tasks as laid down by the present Act. (2) Personal data may be processed only in cases specifically provided for by statute or some other regulation and only to such extent as is in line with the purpose for which the data were collected. Further processing of the said data shall be permitted only if it is not incompatible with the purposes for which the data were collected and if the competent authorities are authorised to process such data for such other purpose in accordance with the law and such processing is necessary and proportionate to that other purpose. (3) Processing of personal data concerning health or sex life shall be permitted only exceptionally if a criminal offence punishable by five years' imprisonment or a more severe penalty could not be detected or proven in any other way or where this would involve disproportionate difficulties.(4) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership shall not be allowed. (5) Personal data collected for the purpose of criminal proceedings may be transmitted to state administration bodies in accordance with a special act and to other legal persons only if the State Attorney's Office or the court determines that such data are required by them for a purpose laid down by law. Upon transmission, the said legal persons shall be warned that they have a duty to implement measures for the protection of data relating to the data subject. (6) The personal data referred to in paragraph 1 of this Article may according to regulations be used in other criminal proceedings, in other proceedings for punishable acts in the

[44] E.g.: Constitutional Court, U-III-4567/2017, 07.2.2018; Supreme Court of Republic of Croatia, I Kž-191/16-5, 13.4.2016.
[45] Title in original language: Zakon o zaštiti fizičkih osoba u vezi s obradom i razmjenom osobnih podataka u svrhe sprječavanja, istraživanja, otkrivanja ili progona kaznenih djela ili izvršavanja kaznenih sankcija.

Republic of Croatia, and in the framework of international legal assistance in criminal matters and international police co-operation.

Article 187
(1) The need for the storage of data and the accuracy of the data kept in the registers of automated processing systems and other registers shall be reviewed every five years. Inaccurate data or data collected in violation of the provisions of Articles 186 and 188 of the present Act shall be rectified or erased without delay.
(2) Unless provided otherwise by a separate act, access to data on a person's identity shall not be permitted: 1) if the proceedings ended with a judgment of conviction, upon expiry of no more than ten years from the moment the sentence was executed, and if no sentence or a suspended sentence was pronounced, from the moment the judgment of conviction became final; 2) if the crime report was dismissed or the proceedings ended with a judgment of acquittal, a judgment of refusal, or were stopped, upon expiry of no more than three years from the moment the decision became final; 3) if the proceedings against a minor ended with a final judgment of conviction, no later than two years after the judgment became final; 4) if the crime report against a minor was dismissed or the proceedings ended with a judgment of acquittal, a judgment of refusal, or were stopped, immediately upon the decision becoming final.
(3) Thirty years after the expiry of the time limits referred to in paragraph 2, any directly available data shall be erased. (4) Personal data collected solely on the basis of identity establishment or a body search may, according to regulations, after the end of the criminal proceedings be used solely for the purpose of detecting or preventing a criminal offence.
(5) Personal data serving to establish the defendant's identity, collected by the security intelligence services, may exceptionally be used as evidence in cases involving the following criminal offences:
1) assassination of the most senior state officials (Article 138), punishment of the most serious forms of criminal offences against the Republic of Croatia (Article 155) and terrorism (Article 169), set forth in the Criminal Code (Official Gazette 110/97, 27/98, 50/00, 129/00, 51/01, 111/03, 190/03, 105/04, 84/05, 71/06, 110/07, 152/08, 57/11 and 77/11); 2) terrorism (Article 97), financing of terrorism (Article 98), terrorist association (Article 102), public incitement to terrorism (Article 99), recruitment for terrorism (Article 100), training for terrorism (Article 101), travel for the purpose terrorism (Article 101a), terrorist association (Article 102), punishment of the most serious forms of criminal offences against the Republic of Croatia (Article 351), set forth in the Criminal Code.

Article 188
(1) Unless otherwise prescribed by law, the State Attorney's Office or the court shall inform a person in writing, upon his/her request, of whether their personal data were collected, stored and processed for the purpose of criminal proceedings. The notification cannot be served on the person concerned until the expiry of a one-year time limit from the issuance of the investigation order or the delivery of notice from Article 213, paragraph 2 of this Act. (2) Unless otherwise prescribed by this Act, the provisions of a special act shall apply accordingly to activities involving the use of personal data for the purposes of criminal proceedings.
(….)

Additional provisions:

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

Article 188a
(1) Personal data collected for the purposes of criminal proceedings may under the present Act and special personal data protection regulations be transmitted or made available to the competent authorities of European Union Member States. (2) Under the conditions set forth in the present Act and special personal data protection regulations, personal data referred to in paragraph 1 of this Article may be transmitted or made available to third states and international bodies. (3) All transmissions of personal data shall be logged for the purposes of verification of the lawfulness of the data processing, self-monitoring and ensuring data integrity and security. (4) Logs prepared under paragraph 3 of this Article shall be communicated on request to the competent supervisory authority for the control of data protection.

Article 188b
(1) The competent authorities shall take steps to provide that personal data which are inaccurate, incomplete or no longer up to date are not transmitted or made available to Member States. To that end, the competent authorities shall, as far as practicable, verify the quality of personal data before they are transmitted or made available. Where possible, in data transmissions, available information shall be added to personal data, which enables the receiving Member State to assess the degree of their accuracy, completeness, up-to-dateness and reliability. If personal data were transmitted without request for their transmission, the receiving authority shall verify without delay whether these data are necessary for the purpose for which they were transmitted. (2) If it is subsequently established that personal data transmitted or made available to Member States are incorrect or were transmitted in violation of the provisions of the present Act or special regulations, the competent authority shall notify the recipient without delay, and it shall rectify or erase such data without delay.

Article 188c
(1) During transmission of personal data pursuant to Article 188a, paragraph 1, of the present Act, the competent authority may indicate the time limits for the retention of transmitted data, upon the expiry of which the recipient must erase or disable access to such data, or review whether or not there is still a need for their use. Exceptionally, this obligation shall not apply if at the time of expiry of stated retention time limits the data delivered are required for the prosecution of criminal offences or the enforcement of criminal penalties. (2) Where during transmission of personal data the competent authority has not indicated a time limit for the retention of data in accordance with paragraph 1 of this Article, the time limits for the retention of data provided for under the national law of the receiving Member State shall apply.

Article 188d
(1) Personal data received from or made available by the competent authority of another European Union Member State may be processed by the competent authorities only if so provided by the present Act or special personal data protection regulations and only for the purpose for which the data were collected. (2) Subject to conditions laid down in Article 186, paragraph 2, of the present Act, personal data referred to in paragraph 1 of this Article may be further processed only for the following purposes: 1) the prevention, detection or prosecution of criminal offences or the execution of criminal penalties; 2) judicial or other proceedings directly related to the prevention, detection or prosecution of criminal offences or the execution of criminal penalties; 3) the prevention of an immediate and serious threat to public security; or 4) any other purpose but only with the prior authorisation of the transmitting Member State or with the consent of the data subject.

(3) The competent authorities may also process personal data referred to in paragraph 1 of this Article for historical, statistical or scientific purposes, provided that they provide appropriate measures for the protection of such data.
(4) The competent authority of the recipient Member State shall, on request, inform the authority which transmitted to it the personal data about their processing.

Article 188e
Where specific personal data processing restrictions apply to personal data exchanges between competent authorities within a Member State, the competent authority shall inform the recipient competent authority of another Member State of such restrictions. The recipient competent authority of a Member State shall ensure that when processing the transmitted data, these processing restrictions are met.

Article 188f
(1) Personal data transmitted or made available by the competent authority of another Member State may be transferred to states that are not member states of the European Union or international bodies only if:
1) it is necessary for the prevention, detection or prosecution of criminal offences or the execution of criminal penalties; 2) the receiving authority in the third state or receiving international body is responsible for the prevention, detection or prosecution of criminal offences or the execution of criminal penalties; 3) the Member State from which the data were obtained has given its consent to the transfer of personal data in compliance with its national law and 4) if the state that is not a European Union Member State or international body concerned ensure an adequate level of protection for the intended data processing.
(2) Exceptionally, if the Member State from which the data were obtained has not given its consent to their transfer (paragraph 1, item 3 of this Article), the transfer of the data referred to in paragraph 1 of this Article to states that are not European Union Member States or international bodies shall be permitted only if their transfer is essential for the prevention of an immediate and serious threat to public security of a Member State, or to essential interests of a European Union Member State, provided the prior consent could not be obtained in time. The competent authority of the Member State from which the data were obtained shall be informed without delay of the transfer without prior consent.
(3) Exceptionally, personal data referred to in paragraph 1 of this Article may be transferred to states that are not European Union Member States or international bodies that do not ensure an adequate level of protection for the intended data processing (paragraph 1, item 4 of this Article), if the national law of the Member State transferring the data so provides because of legitimate specific interests of the data subject or legitimate prevailing interests, especially important public interests, or if the receiving state or international body provides safeguards which are deemed adequate by the national law of the Member State from which the data originate.
(4) The adequacy of the level of protection referred to in paragraph 1, item 4 of this Article shall be assessed in the light of all the circumstances surrounding personal data transfer operations. The assessment shall give particular consideration to the nature of the data, the purpose and duration of processing, the state of origin and the state or international body of final destination of the data, the rules of law, both general and specific, in force in the receiving state or international body, and the applicable professional rules and security measures.
(5) The recipient of personal data referred to in paragraph 1 of this Article shall, on request, inform the authority which transmitted to it the personal data about their processing.

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

Article 188g
(1) Personal data transmitted or made available by the competent authority of another Member State may be transmitted to private parties only if: 1) the competent authority of the Member State from which the data were obtained has consented to transmission in compliance with its national law; 2) there are no legitimate specific interests of the data subject prevent transmission; and 3) transfer is necessary for the performance of tasks lawfully assigned to the competent authority, or for the prevention, detection or prosecution of criminal offences or the execution of criminal penalties, the prevention of an immediate and serious threat to public security or the prevention of serious harm to the rights of individuals.
(2) The competent authority transmitting the data to a private party shall inform the latter of the purposes for which the transmitted data may be used. (3) The recipient of personal data referred to in paragraph 1 of this Article shall, on request, inform the authority which transmitted to it the personal data about their processing.

Personal data protection in search (Article 249/3)

Personal data obtained by a search may only be used for the purposes of criminal proceedings and shall be erased without delay when this purpose ceases to exist.

Data protection in acquiring, recording, protecting and storing of data (Article 263)

In acquiring, recording, protecting and storing of data stored in computers and devices connected thereto, as well as in devices used for collecting and transferring data, data carriers, subscription information in the possession of a service provider, pursuant to Article 263 of the CPA in connection with Article 261 (temporary seizure), special attention shall be paid to rules on the confidentiality of certain data (Articles 186 through 188).

Unlawful evidence and data protection (see Article 10 of the CPA)

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) In the area of criminalistic activities, provisions of the Police Duties and Powers Act (PDPA)[46] that might imply police authority of preliminary reading/examination of the mobile device (as objects) by the police (prior to and outside of the evidentiary actions of seizure/search regulated by the Croatian Criminal Procedure Act - CPA[47]): Articles 75-77 (examination / inspection, which must be suspended if it reveals traces of a criminal offense that is prosecuted ex officio or other evidence, following which, if necessary, provisions on search under the CPA shall be followed).[48] No pertinent case law found nor literature specifying concrete application of

[46] Title in original language: Zakon o policijskim poslovima i ovlastima (Official Gazette no. 76/09, 92/14 and 70/19).

[47] Title in original language: Zakon o kaznenom postupku (Official Gazette no. 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17, 126/19 and 126/19).

[48] Article 75 of the PDPA: (1) A police officer may examine persons, objects and means of transport when: 1. the escape of the perpetrator of a criminal offense prosecuted ex officio or a misdemeanor should be prevented, 2. it is necessary to discover traces or objects that may be used to establish the facts of a criminal offense or misdemeanor, 3. it is necessary for the protection of general safety. (2) Article 71, paragraphs 2 and 3 of this Act shall apply accordingly when performing the examination.
Article 71: (2) Classified data may be inspected by a police officer only under the conditions and in the manner stipulated by the law. (3) The person whose business documents are being inspected may request that the data pertaining to his business activities not be published. Article 76: (1) The examination of a person shall be performed by a person of the same sex. Exceptionally, when an urgent examination of a person is necessary in order to confiscate weapons or objects suitable for attack or self-harm, the examination may be performed by a person of the opposite sex. (2) During the examination, the police officer may use technical means and an official dog. (3) Unless otherwise prescribed by a special law, when undertaking an examination, a police officer may forcibly open a closed

those provisions to mobile devices/data. Temporary seizure of objects – the PDPA: in early stages where police criminalistic activities are concerned, according to available literature Article 59 of the PDPA on temporary seizure applies also to computer data.[49] However, no case law was found nor further literature specifying concrete application of that and related provisions to mobile devices/data.[50]

b) In the area of criminalistic activities, provisions of the PDPA and the *Code of Practice of Police Officers*[51] on covert police actions (e.g. observation, following, traps, disguised collecting of information on the computer system) might imply police authority of preliminary reading/examination of the mobile device/data by the police. No pertinent case law found and/or literature specifying application of those provisions to mobile devices/data. All relevant

---

means of transport or disassemble an object carried by a person only if there is an imminent danger to human life or property or to apprehend the perpetrator. If necessary, an expert will be invited to enable an examination.
Article 77: (1) The examination of objects and means of transport shall be suspended, if the examination reveals traces of a criminal offense that is prosecuted ex officio or other evidence, or where it is necessary to forcibly open or disassemble the object of examination. (2) After the suspension of the examination, if necessary, the provisions on search from a special law shall be followed. (3) Before undertaking the search referred to in paragraph 2 of this Article, the police officer shall inform the State Attorney and act upon his/her order. (4) The police officer shall compile a report on the actions referred to in Articles 75 and 76 of this Act and issue appropriate certificates. In the report, the police officer will specifically explain the reasons for the examination performed by a person of the opposite sex.

[49] Petar Veić, Igor Martinović, Izazovi policijskog postupanja u otkrivanju i dokazivanju računalnog kriminala (researcher's translation into English: Challenges of police action in detecting and proving computer crime), Proceedings of the 5th International Scientific and Professional Conference, the Police College Research Days in Zagreb, New Technologies and Methods Used for Improvement of the Police Role in Security Matters, Zagreb, Croatia, 21.-22.4.2016, p. 421.

[50] Article 58: (1) A police officer shall temporarily seize and keep objects under the conditions and in the manner stipulated by this Act and other laws. (2) The police officer shall issue a receipt on temporary seizure of objects. Article 59: A police officer shall also temporarily seize an object if: 1. it is likely that the object was intended for use in committing a criminal offence prosecuted ex officio or a misdemeanour, or that it was obtained by committing a criminal offence prosecuted ex officio or a misdemeanour, unless the criminal offenses are that of insult or defamation, 2. this is necessary for maintaining public safety, 3. the object may be used for self-injury, assault, escape, and for concealing or destroying traces of a criminal offence prosecuted ex officio or a misdemeanour, 4. stipulated by a special regulation. Article 60: (1) When the keeping of temporarily seized objects in police premises is not possible or if it is connected with substantial difficulties, such objects may be kept in another place, until a decision is issued by the competent body, unless otherwise stipulated by another act. (2) When the reasons for temporarily seizing the object are no longer present, the object shall be returned to the person from whom it was temporarily seized, unless otherwise stipulated by the law or a decision by the competent body. (3) Temporarily seized objects obtained by the commital of a criminal offence that is prosecuted by private motion shall be returned to their owner at their request.

[51] Title in original language: Pravilnik o načinu postupanja policijskih službenika (Official Gazette no. 89/10 and 76/15).

provisions should be interpreted and applied according to specific circumstances of each case (mobile device not seized scenarios).[52]

c) Accessing data directly from other sources such as a server under the provisions of the Criminal Procedure Act – CPA[53], e.g. where data from mobile phone are also stored on company server: search of server: Article 257 on search of a movable and general search provisions where applicable (Articles 240-250); temporary seizure of „data stored in computers and devices connected thereto, as well as in devices used for collecting and transferring data, data carriers and subscription information in the possession of a service provider" (Article 263 in connection with Articles 261-262 of the CPA).

[52] Under Article 12 of the PDPA, covert police actions apply also to means of communication. Article 80 of the PDPA: (1) The police may take covert police actions during criminalistic investigation if it is obvious that other actions would not achieve the goal of policing. (2) Covert police actions are: 1. observation, 2. following, 3. trap, 4. entrapment. (3) Covert police actions of observation and following may last fifteen days from the issuance of the order, and for the purpose of successful execution of police work they may be extended for another fifteen days. (4) A written order for the taking of covert police actions of observation and following, the content and duration thereof is issued by the Director General or a person authorized by him/her, and in case of extension the order may only be issued by the Director General or the person replacing him/her. (5) As an exception to paragraph 4 of this Article, when circumstances require urgency of action, an order can be given orally, but it must be confirmed in writing no later than 24 hours after an oral order was issued. (6) Covert police actions of traps and entrapments shall be undertaken on the basis of the order of the Chief of the Directorate in the Police Directorate, Chief of the National Police Office for the Suppression of Corruption and Organized Crime, the Chief of police administration and the Chief of the police station or a person authorized by them, and may last as long as there are reasons for their application. (7) On conducted covert police actions of observing and following, in order to monitor the legality of their implementation, the competent State Attorney and the Director General shall be notified within the time limit of 48 hours from the completion of the action. Article 39 of the Code of Practice of Police Officers: A police officer may with disguise collect information also on the computer system, either by opening an account, or with written consent of the user of existing account. The police officer shall submit an operational report or official note on the collected data. Article 122 of the Code of Practice of Police Officers: A police officer who intends to apply covert police trapping and entrapment actions, prior to their implementation, shall compile an Implementation Plan. A record on the setting up of a trap shall be made on the conducted covert police operation of the trap. Before conducting the trap, the police officer is obliged to submit to the competent State Attorney the record on receipt of the criminal report or a special report showing the grounds for suspicion that a criminal offense was commited which is prosecuted ex officio and the record on the setting up of a trap. Article 123 of the Code of Practice of Police Officers: The record on the setting up of a trap must contain the following information: - identification data (mark, type, factory number, serial number, etc.) and description of the object to be used in the carrying out of the trap, - the method of covert marking of the object that will be used in conducting the trap. The record referred to in paragraph 1 of this Article may be accompanied by a technical recording of the object used to conduct the trap. By way of derogation from paragraph 1 of this Article, if the trap is set in a computer system or online, the record on the setting up of a trap shall contain information on computer programs to be used and information on the way that they would be used. Article 124 of the Code of Practice of Police Officers: An object owned by the injured party shall be used to set the trap, and exceptionally an object that can be secured by the police can also be used. The police officer may equip the object referred to in paragraph 1 of this Article with a device for monitoring the transfer of the object.

[53] Title in original language: Zakon o kaznenom postupku (Official Gazette no. 152/08, 76/09, 80/11, 121/11, 91/12, 143/12, 56/13, 145/13, 152/14, 70/17, 126/19 and 126/19).

d) Pre-trial phases/measures regulated by the CPA, during the taking of which it is possible to conduct search and/or seizure - see circumstances for conducting inquiries into criminal offences (Article 207); circumstances for conducting urgent evidentiary actions (Article 212); circumstances for conducting evidentiary actions when the perpetrator is unknown (Article 214).

e) Case law examples: photographing mobile device owned by witness / injured party and contents thereof with consent of owner (cases available in Researcher's overview).

f) Secret interception, collection, and recording of computer data: special evidentiary actions temporarily restricting certain constitutional rights of citizens under the CPA: where inquiries into criminal offenses cannot be carried out otherwise or where this would entail disproportionate difficulty, against suspects for specific offenses and connected persons (measures in respect to other people's objects with written consent), with reasoned written warrant (details in Articles 332-338 of the CPA).

g) Accessing non-content mobile data from operators: a) checking establishment of contact by means of telecommunication for a registered owner/user (Article 339a of the CPA - only for specific criminal offenses and offences punishable by imprisonment for a term of more than five years); b) verification of contact by electronic communications - Article 68 of the Police Duties and Powers Act (in connection with Article 207 of the CPA on inquiries into criminal offenses).

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?*

In addition to conditions for the taking of each individual measure stipulated above (when can a certain measure be taken – limits defined by measure itself):

a) For the police criminalistic activity of examination / inspection under the PDPA

Article 71/2-3 of the PDPA
(2) Classified data may be inspected by a police officer only under the conditions and in the manner stipulated by the law. (3) The person whose business documents are being inspected may request that the data pertaining to his business activities not be published.

Article 77/1 of the PDPA
The examination of objects and means of transport shall be suspended, if the examination reveals traces of a criminal offense that is prosecuted ex officio or other evidence, or where it is necessary to forcibly open or disassemble the object of examination.

b) Data protection rules in the CPA (Article 186) - general application for all CPA measures

(1) Personal data may be collected by the competent authorities only for purposes specified by law in the framework of their tasks as laid down by the present Act. (2) Personal data may be processed only in cases specifically provided for by statute or some other regulation and only to such extent as is in line with the purpose for which the data were collected. Further processing of the said data shall be permitted only if it is not incompatible with the purposes for which the data were collected and if the competent authorities are authorised to process such data for such other purpose in accordance with the law and such processing is necessary and proportionate to that other purpose. (3) Processing of personal data concerning health or sex life shall be permitted only exceptionally if a criminal offence punishable by five years' imprisonment or a more severe penalty could not be detected or proven in any other way or where this would involve disproportionate difficulties. (4) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership shall not be allowed. (…)

c) Limits defined by the search warrant (Article 242/1 of the CPA)

Unless otherwise prescribed by this Act, at the request of the State Attorney the judge of investigation shall order a search by a written warrant including a statement of reasons. The search warrant shall contain the following: 1) designation of the object of search (person, home, other premises or movables); 2) purpose of the search; 3) authority conducting the search.

d) Limits to seizure during search (Article 248(2) of the CPA))

Only such objects and documents that are related to the purpose of a search, as well as the objects specified in Article 249, paragraphs 1[54] and 2[55] of this Act shall be temporarily seized during the search.

e) Personal data protection in search (Article 249/3 of the CPA)

Personal data obtained by a search may only be used for the purposes of criminal proceedings and shall be erased without delay when this purpose ceases to exist.

[54] If during a search objects not related to the criminal offence for which a search warrant was issued are found, however, which objects point to the commission of another criminal offence prosecuted *ex officio*, the said objects shall be described in the minutes and temporarily seized and a seizure receipt shall be immediately issued. The State Attorney shall be immediately notified thereof.

[55] Where the State Attorney establishes that there is no ground for instituting criminal proceedings and where there is no other statutory ground for the seizure of the objects concerned, the said objects shall be immediately returned, of which minutes shall be drafted. The objects used during search of a computer and similar devices shall be returned to their users after the search, provided they are not necessary for the further conduct of criminal proceedings.

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

f) Limits prescribed for the measure of temporary seizure of data stored in computers and devices connected thereto, as well as in devices used for collecting and transferring data, data carriers and subscription information in the possession of a service provider (Article 263/3 of the CPA):

In acquiring, recording, protecting and storing of data special attention shall be paid to rules on the confidentiality of certain data (Articles 186 through 188). Depending on the circumstances, data that are not related to the criminal offence for which proceedings are undertaken, but which are needed by the person against whom the measure in question has been taken, may be recorded onto an appropriate medium and returned to this person also prior to the conclusion of proceedings.

g) Exceptions to temporary seizure (Article 262 of the CPA)

h) Limits defined by written reasoned warrant for special evidentiary measures (Article 335/1 of the CPA)

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

/With the understanding of this question, that "allowed" does not mean that information collected by such measure would be "allowed" as evidence in court proceeedings/: whether such tools can be used or not is not expressly prescribed in legal provisions (examination/inspection) where police activities are concerned. I would assume yes, however, answer should best be provided by authorities working in the field.

Where covert data gathering is concerned as part of early police criminalistic activity, Article 39 of the Code of Practice of Police Officers specifies that the police may with disguise collect information on the computer system, either by opening an account, or with written consent of the user of existing account.

Where the action of search of a movable under Article 257 of the CPA applies, there is a prescribed duty to enable access and enable unhindered use/accomplishment of search aims (e.g. passwords, encryption): at the request of the authority conducting a search, the person using a computer or having access to a computer or another device or data carrier, as well as a telecommunications service provider shall enable access to a computer, device or data carrier and shall provide the necessary information for unhindered use and achievement of the goals of the search. Where they do not comply, despite there being no justifiable reasons therefore, they may upon the motion of the State Attorney be punished by the judge of investigation (monetary fine

up to 50.000,00 Kuna, and if they fail to comply even further, imprisonment until compliance but no longer than one month). The defendant cannot be punished.

Secret surveillance measures as special evidentiary actions under the CPA (Articles 332 and further) imply by logic the possibility of bypassing security measures, and use of technical means to implement such measures are envisaged in the Ordinance on the manner of conduct of special evidentiary actions (Official Gazette 102/09 – see Researcher's overview). The operative and technical centre for telecommunications supervision, which is responsible for ensuring technical coordination with the providers of telecommunication services in Croatia, and the providers of telecommunication services are obliged to provide the necessary technical assistance to the police (duty and fine set out in Article 335/2 of the CPA).

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

That is not specified in provisions on early-stage criminalistic police activity of examination / inspection (Article 75 of the PDPA). Note: examination must be suspended if there are found traces of a criminal offense that is prosecuted ex officio or other evidence, and if necessary, provisions on search from the CPA should thereon apply (Article 77/1-2 of the PDPA). Also in early stages where police criminalistic activities are concerned, according to literature Article 59 of the PDPA on temporary seizure applies to computer data as well.[56] While seizure of mobile data would as a measure imply also the copying/recording of data, concrete details on measure and application thereof to such data in the context of Article 59 of the PDPA are not available. Clear answers should therefore be provided by authorities working in the field.

Where seizure provisions of Article 263 of the CPA apply, data must be handed over and data may be recorded (temporary seizure of data stored in computers and devices connected thereto, as well as in devices used for collecting and transferring data, data carriers and subscription information in the possession of a service provider - Article 263, in connection with Articles 261-262 of the CPA).

Copying in cases of photographying mobile phone and contents with consent of witnesses - case law examples: a) the Supreme Court affirmed the decison of the court of first instance allowing as evidence the photography of the accused in form of a contact in the mobile phone of the witness, made by police officers, and the corresponding CD. According to the Court, the warrant

[56] Petar Veić, Igor Martinović, Izazovi policijskog postupanja u otkrivanju i dokazivanju računalnog kriminala (researcher's translation into English: Challenges of police action in detecting and proving computer crime), Proceedings of the 5th International Scientific and Professional Conference, the Police College Research Days in Zagreb, New Technologies and Methods Used for Improvement of the Police Role in Security Matters, Zagreb, Croatia, 21.-22.4.2016, p. 421.

of the judge of investigation was not necessary for such action of the police, since the witness on her own and voluntarily read out the contents of her mobile phone on the contact with the accused and voluntarily handed her mobile phone to the police officers so that they could make a photography of that contact.[57]; b) Mobile device of a witness had not been seized by the police and no search of a mobile phone was conducted. The police photographed the phone as well as the data contained in it (specifically: photographs made in a public space). All this was voluntarily provided and made available to the police by the witness - owner of device. The Supreme Court rejected the defendant's appeal and affirmed the decision of the court of first instance rejecting the claim for exclusion of such evidence (photographs) as unlawful under Article 10 (paragraph 2, item 3)[58] of the CPA. More cases are available in Researcher's overview (with a disclaimer that many decisions covered relate to claims on exclusion of evidence, with main proceedings still ongoing and/or final court decisions in the case not being final yet).

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

According to case law yes for cases of photographying mobile phone owned by witness/injured party and contents (unless other criminal procedural phase and related provision applies - e.g. duty to provide data and enable search in the context of device/data seizure, and search of device, see above). Consent requirement is not visible from the provisions on early-stage criminalistic police activities of: examination /inspection (Article 75 of the PDPA); temporary seizure (Article 59 of the PDPA). Where covert data gathering on the computer system is concerned as part of police criminalistic activity, Article 39 of the Code of Practice of Police Officers specifies that the police may with disguise collect information on the computer system, either by opening an account, or with written consent of the user of existing account.

Clear answers should be provided by authorities working in the field.

No - where the action of search of a movable under Article 257 of the CPA applies. At the request of the authority conducting a search, the person using a computer or having access to a computer or another device or data carrier, as well as a telecommunications service provider shall enable access to a computer, device or data carrier and shall provide the necessary information for unhindered use and achievement of the goals of the search. Where they do not comply, despite there being no justifiable reasons therefore, they may upon the motion of the State Attorney be punished by the judge of investigation (monetary fine up to 50.000,00 Kuna, and if they fail to comply even further, imprisonment until compliance but no longer than one month). The defendant cannot be punished.

[57] Supreme Court of the Republic of Croatia, decision, I Kž-Us 28/2020-4, 09.4.2020.
[58] Evidence was not "obtained in violation of criminal procedure provisions which is expressly provided for in the Criminal Procedure Act".

No - where rules on temporary seizure of computer/mobile phone data under Article 263 of the CPA applies. According to that provision the data must be handed in an integral, original, legible and understandable form. In the case of refusal to hand over data, it may be proceeded in accordance with Article 259, paragraph 1, of this Act, which means that a monetary fine may be issued against the person up to 50.000,00 Kuna, and if he/she fails to comply even further, he/she may be imprisoned until compliance but no longer than one month. The punishment applies neither to the defendant nor to persons exempted from the duty to testify. The data holder shall be warned of the consequences resulting from non-compliance with the request to hand over the data (Article 261, paragraph 2).

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

That is not specified in provisions on early-stage criminalistic police activity of examination / inspection (Article 75 of the PDPA). Where provisions of the CPA apply on search of a movable (Article 257), no, but sanctions are prescribed in case of refusal to unlock the device, which do not aply to the defendant.[59]

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

There is no reference to such duty specifically in relation to early-stage criminalistic police activity of examination / inspection of the mobile device under Article 75 of the PDPA. According to Article 77, paragraph 4 of that act, the police officer shall draw up a report on examination conducted and issue appropriate certificates.

Notification on search carried out under the CPA (device owner in capacity of the defendant)[60]
Handing of search warrant and prior invitation to voluntarily hand over the device under the CPA - Article 243 of the CPA

[59] At the request of the authority conducting a search, the person using a computer or having access to a computer or another device or data carrier, as well as a telecommunications service provider shall enable access to a computer, device or data carrier and shall provide the necessary information for unhindered use and achievement of the goals of the search. Where they do not comply, despite there being no justifiable reasons therefore, they may upon the motion of the State Attorney be punished by the judge of investigation (monetary fine up to 50.000,00 Kuna, and if they fail to comply even further, imprisonment until compliance but no longer than one month). The defendant cannot be punished.

[60] With the serving of the search warrant the defendant shall be notified of his/her rights, such as on information on what he/she is being charged with and the circumstances giving rise to reasonable grounds for suspicion against him/her (unless he/she had already received the investigation order), the right to inspect the case file (exception – Article 184a), that he/she is not obliged to present his/her defense or answer questions, on the right to use his/her own language and on right to an interpreter, on the right concerning defense counsel (details in Article 239 of the CPA).

Exceptions (no prior handing of warrant, instruction on rights or invitation to hand over the device) - Articles 244-245 of the CPA
Minutes (protocol) of the search + seized objects/documents + receipt on seized objects - Article 248 (1, 3) of the CPA

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

Answer is here provided in understanding that this question does not include warranted formal search of mobile device under the CPA (as opposed to same question for the next group of questions where mobile device has been formally seized under the CPA).

No particular formal requirements are specified for the early-stage criminalistic police activity of *examination / inspection* under Article 75 of the PDPA.

General rule under the CPA on State Attorney's authorization to order the police the conduct of inquiries and the taking of other measures for the purpose of collecting information required for deciding on the crime report (Article 206h, paragraph 1 of the CPA).[61]

Prescribed requirements for conduct of inquires into criminal offences (Article 207 of the CPA): no warrant prescribed but the police must inform the State Attorney of undertaken inquiries.[62]

Police authority without State Attorney's prior - prescribed requirements for search and seizure by the police in the scope of urgent evidentiary actions (where there is risk of delay, before

[61] Under Article 206h, paragraph 1 of the CPA, the State Attorney may order the police to gather the necessary information by conducting inquiries and taking other measures for the purpose of collecting information required for deciding on the crime report (note: "other measures" are not specified). In his/her order the State Attorney may specify the contents of the inquiry or measure as well as order that the police inform him/her immediately of the inquiry conducted or the measure taken. If the State Attorney orders that he/she be present at the inquiry or the taking of a measure, the police shall conduct the inquiry or take the measure in a manner which allows for his/her presence. The police is required to proceed as ordered by the State Attorney and unless the State Attorney orders otherwise, it shall inform the State Attorney of the inquiries conducted or the measures taken no later than thirty days from receipt of the order.

[62] According to paragraph 1 of that Article, if there are grounds for suspicion that a criminal offence prosecuted ex officio was committed, police has the right and duty to take necessary measures to: 1) find the perpetrator of the criminal offence, to prevent the perpetrator of or the participant in a criminal offence from going into hiding or fleeing; 2) discover and secure the traces of a criminal offence and objects that may be used for establishing the facts; and 3) collect all information that might be useful for the successful conduct of criminal proceedings. Note: "necessary measures" are here not specified. Paragraphs 2 and 3 are, as follows: (2) The police shall inform the State Attorney in due time of the inquiries undertaken into criminal offences. If the State Attorney informs the police of his or her intention to be present at the conduct of particular inquiries or the taking of particular measures, the police shall conduct the inquiries or take the measures in a way that allows for such State Attorney's presence. (3) On the facts and circumstances established during the taking of the actions referred to in paragraphs 1 and 2 of this Article, which facts and circumstances might be of interest for the criminal proceedings, the police shall draw up an official note (…)".

institution of criminal proceedings), for criminal offenses: 1) punishable by imprisonment for up to five years; 2) punishable by imprisonment of ove five years.[63]

Search without a warrant – inspection of the scene of commission of a criminal offence prosecuted ex officio (Article 246/1).[64]

In cases where data can be accessed from other sources such as server, under the provisions of the CPA (e.g. where data from mobile phone are also stored on company server): see Article 257 of the CPA on search of a movable and the general search provisions, depending on applicability (Articles 240-250). As a rule (unless otherwise prescribed by the CPA, e.g. for cases in Articles 245, 246, etc.) the judge of investigation shall at the State Attorney's request order a search by a written warrant including a statement of reasons. Contents of search warrant are: 1) designation of search object (person, home, other premises or *movables)*; 2) search purpose; 3) authority conducting the search.
In other cases of searches that may lead to seizure of a mobile device, there are prescribed exceptions to mentioned warrant and stipulated conditions (e.g. urgent search of a person and means of transport – details in Article 245 of the CPA), and other (e.g. Article 246, and other CPA rules (…)).

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

Where the CPA is concerned only the defendant cannot be sanctioned in case of refusing to comply with the order under Article 257 (search of a movable i.e. mobile device). In cases of refusing to hand over computer data under Article 263 only the defendant and the persons exempted from the duty to testify shall not be punished if they refuse to hand over computer data.

[63] Article 212, paragraph 1 of the CPA: (1) Where there is a risk of delay, the police may, even before the institution of criminal proceedings for criminal offences punishable by imprisonment for a term of up to five years, conduct searches (Article 246), temporarily seize items (Article 261) (…). (2) In the case of criminal offences punishable by imprisonment for a term of over five years, the police shall inform immediately the State Attorney of any risk of delay or the need to collect evidence, except where the acts of collection of evidence concern temporary seizure of items (Article 261) or searches (Article 246). The State Attorney may perform the evidence-collecting acts referred to in paragraph 1 of this Article himself/herself or may leave it to the police or order the investigator to perform them. The State Attorney who arrives at a location where an inspection or a search is underway may take over the performance of the act. (…) (5) The police shall inform the State Attorney without delay of the results of acts performed by it under paragraphs 1 and 2 of this Article.

[64] The State Attorney, the investigator or the police conducting inspection of the scene of commission of a criminal offence prosecuted ex officio may conduct a search without a warrant immediately and no later than eight hours after the criminal offence is detected, if that is absolutely necessary for averting a danger to the lives and health of people or to property of considerable value or for securing any traces or evidence directly related to the criminal offence giving rise to the inspection, unless the search in question is a search of the home or premises referred to in Article 256 of the present Act.

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.*

With consent (e.g. provided password) the data may be accessed, otherwise EIO/MLATs are used. According to Ministry of Interior's Report for 2019, during 2018 a total of 209 requests were processed from various organizational units of the police (Ministry of the Interior) for the cross-border acquisition of electronic evidence from various Internet service providers operating outside of the Republic of Croatia.[65]
According to the 2017 Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" – Report on Croatia:

> "In some cases, police officers use the services which some providers of electronic services provide to the police authorities to communicate and to ensure a faster and more effective response to, for example, the exploitation of children for pornography (e.g. Facebook, Skype, and Instagram Law Enforcement Response Team). International police co-operation with the police authorities in some countries (e.g. United States, Australia, New Zealand, etc.) has also been very successful in cases involving sexual abuse and exploitation of children."[66]

Available data on *Government requests for customer data from foreign ISP's* such as Facebook, Google, etc. can be found in *transparency reports* from internet service providers.[67]
Some data is also available in the recent *Cybercrime Convention Committee report: The Budapest Convention on Cybercrime: benefits and impact in practice.*[68]

---

[65] Ministry of the Interior, Report on work for 2019 (title in original language: Izvješće o radu za 2019. godinu), https://mup.gov.hr/UserDocsImages/dokumenti/2019/STUDENI/Godisnje%20izvjesce%20o%20radu%20Ministarstva%20unutarnjih%20poslova.pdf, p. 59.
[66] Council of the European Union, Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime"- Report on Croatia, 5250/1/17, REV 1 DCL 1, GENVAL3 CYBER9, Brussels,11.4. 2017, https://data.consilium.europa.eu/doc/document/ST-5250-2017-REV-1-DCL-1/en/pdf, p. 86.
[67] E.g. Facebook: https://govtrequests.facebook.com/about/# Google https://www.google.com/transparencyreport/; Microsoft https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report; Apple http://www.apple.com/privacy/transparency-reports/.
[68] See Requests for account information received/disclosed by Facebook, Google/YouTube and Microsoft/Skype, in: Cybercrime Convention Committee (T-CY), The Budapest Convention on Cybercrime: benefits and impact in

For more details and suggestions on national contact points for obtaining relevant information on specific practices in this area, please see Section 6 - Comments.

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

Due to numerous measures of gathering information that may apply throughout different phases of -proceedings (and even according to different rules) one needs to closely look at each concretely applicable measure in relation to the concrete offense and phase of proceedings. Certain measures can only be applied in respect of certain criminal offenses (see, e.g. Article 332, 339a of the CPA), there are prescribed requirements for the conduct of inquires into criminal offences (if there are grounds for suspicion that a criminal offence prosecuted ex officio was committed - see Article 207 of the CPA), there are prescribed requirements for search and seizure conducted by the police in the scope of urgent evidentiary actions, for criminal offenses that are: 1) punishable by imprisonment for up to five years; 2) punishable by imprisonment of ove five years (see Article 212, paragraph 1 of the CPA), etc.

15. *Does not following the applicable rules always lead to inadmissibility in court of the evidence in this scenario?*

"Mobile phone not seized" data related answers:
Often times where the police makes an official note on conducted pre-trial activities, measures and gathered information, results of measures and/or gathered data would not be included into court files as evidence. Where it is not expressly stated in the CPA that collected objects/data during pre-trial phases may or may not be used as evidence, there is lack of certainty as to their probative value in court, as it will depend on court practice (eg. ex officio exclusion / exclusion on the basis of submitted claim). For example, the CPA expressly prescribes that objects seized in violation of Article 262, paragraph 1 of the CPA (prescribing what cannot be seized) cannot be used in evidence in criminal proceedings (Article 262/7). Also, it prescribes that recordings (and documents and objects) obtained by, i.a., interception, collection, and recording of computer data under Article 332 of the CPA (special evidentiary actions temporarily restricting constitutional rights) may be used as evidence in criminal proceedings (Article 333/1). However, where such actions are taken in violation of Article 332 of the CPA, evidence learned from the data thus collected may not be used as evidence in proceedings (Article 335/7). CPA rules on legality of

practice, T-CY (2020)16, Strasbourg, 13 July 2020, https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac, p. 23.

evidence and related case law are provided in answers to relevant questions (Section 3 - admissibility of evidence before courts), also see Researcher's overview.

Mobile device seized

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

Yes

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

Temporary Seizure under the CPA

Circumstances, duty to hand over and sanction (exceptions): Article 261

(1) Objects that are to be seized under the Criminal Code[69] or which may serve to establish facts in proceedings shall be temporarily seized and their safekeeping shall be ensured.
(2) Whoever is in possession of such objects shall be required to hand them over at the request of the State Attorney, the investigator or the police. The State Attorney, the investigator or the police shall warn the holder of such an object of the consequences resulting from non-compliance with the request.
(3) A person who for no justified reason fails to comply with the request to hand over objects may, upon a reasoned motion of the State Attorney, be punished by the judge of investigation pursuant to Article 259, paragraph 1 of this Act.[70]
(4) The measures referred to in paragraph 2 of this Article shall apply neither to the defendant nor to the persons exempt from the duty to testify (Article 285).

Who can order: State Attorney, the investigator or the police (261/2)

[69] Under Article 79 of the Criminal Code on confiscation of objects: (1) The objects and means which are the product of a commission of a criminal offence shall be confiscated. (2) The court may confiscate the objects and means that were intended for use or were used in the commission of a criminal offence. (3) The objects and means referred to in paragraphs 1 and 2 of this Article may be confiscated even when the perpetrator of the wrongful act is not guilty.
[70] In such cases a monetary fine shall be issued against him/her up to 50.000,00 Kuna, and if he/she fails to comply even further, he/she shall be imprisoned until compliance but no longer than one month.

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

Ban on temporary seizure of certain objects, documents and recordings; and exceptions from this ban (Article 262 / 1-5)

Temporary seizure: minutes and receipt (Article 262 / 6)

A receipt is issued for temporarily seized objects.

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

Yes as a rule with a search warrant.

Article 257 of the CPA on search of a movable, general search provisions - depending on applicability (Articles 240-250: Researcher's overview).

Article 257:
(1) A search of movables shall also include a search of a computer and devices connected therewith, of other devices intended for collecting, saving and transferring data, for telephone, computer and other kinds of communication, and of data carriers. At the request of the authority conducting a search, the person using a computer or having access to a computer or another device or data carrier, as well as a telecommunications service provider shall enable access to a computer, device or data carrier and shall provide the necessary information for unhindered use and achievement of the goals of the search.

(2) Upon the order of the authority carrying out a search, the person using a computer or having access to a computer and other devices referred to in paragraph 1 of this Article, and a telecommunications service provider, shall immediately take measures to prevent the destruction or modification of data. The authority carrying out a search may order that an expert assistant take these measures.

(3) The person using a computer or having access to a computer or other device or data carrier, and a telecommunications service provider, who does not comply with the requirements of paragraphs 1 and 2 of this Article, despite there being no justifiable reasons therefore, may, upon the motion of the State Attorney, be punished by the judge of investigation in accordance with the provision of Article 259, paragraph 1, of this Act. The provision on punishment shall not apply to the defendant.

Conditions for *temporary seizure of data* stored in computers and devices connected thereto, as well as in devices used for collecting and transferring data, data carriers and subscription

information in the possession of a service provider are prescribed in *Article 263* (in connection with Articles 261-262 of the CPA).

What can be temporarily seized during search (Article 248(2))

Only such objects and documents that are related to the purpose of a search, as well as the objects specified in Article 249, paragraphs 1[71] and 2[72], of this Act shall be temporarily seized during the search.

Search without warrant – inspection (Article 246)

(1) The State Attorney, the investigator or the police conducting inspection of the scene of commission of a criminal offence prosecuted ex officio may conduct a search without a warrant immediately and no later than eight hours after the criminal offence is detected, if that is absolutely necessary for averting a danger to the lives and health of people or to property of considerable value or for securing any traces or evidence directly related to the criminal offence giving rise to the inspection, unless the search in question is a search of the home or premises referred to in Article 256 of the present Act.
(5) When the police conducts a search in the absence of a search warrant, it shall immediately deliver the protocol of the search and the report to the State Attorney having jurisdiction.

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?*

CPA provisions:

a) *Limits defined by prescribed purpose of search (Article 240)*

[71] If during a search objects not related to the criminal offence for which a search warrant was issued are found, however, which objects point to the commission of another criminal offence prosecuted *ex officio*, the said objects shall be described in the minutes and temporarily seized and a seizure receipt shall be immediately issued. The State Attorney shall be immediately notified thereof.
[72] Where the State Attorney establishes that there is no ground for instituting criminal proceedings and where there is no other statutory ground for the seizure of the objects concerned, the said objects shall be immediately returned, of which minutes shall be drafted. The objects used during search of a computer and similar devices shall be returned to their users after the search, provided they are not necessary for the further conduct of criminal proceedings.

(1) Search means an examination of the object of the search by means of senses and their aids under the conditions and in the manner prescribed by this Act and other regulations.
(2) The search of a home, other premises, means of transport, any other movable or a person shall be conducted for the purpose of finding the perpetrator of a criminal offence, an object or traces important for criminal proceedings, where it is probable that they are located in a specific place, in the immediate surroundings of or on a certain person.
(3) Search regulations shall not apply to natural, public or abandoned premises.

b) Limits defined by the search warrant (242/1 of the CPA)

Unless otherwise prescribed by this Act, at the request of the State Attorney the judge of investigation shall order a search by a written warrant including a statement of reasons. The search warrant shall contain the following: 1) designation of the object of search (person, home, other premises or movables); 2) purpose of the search; 3) authority conducting the search.

c) Prescribed data protection in search (Article 249/3) of the CPA)

Personal data obtained by a search may only be used for the purposes of criminal proceedings and shall be erased without delay when this purpose ceases to exist.

d) Limits to seizure during search (Article 248/2) of the CPA)

Only such objects and documents that are related to the purpose of a search, as well as the objects specified in Article 249, paragraphs 1[73] and 2[74] of this Act shall be temporarily seized during the search.

e) Limits prescribed for the measure of temporary seizure of „data stored in computers and devices connected thereto, as well as in devices used for collecting and transferring data, data carriers and subscription information in the possession of a service provider" (Article 263/3 of the CPA):

> "In acquiring, recording, protecting and storing of data special attention shall be paid to rules on the confidentiality of certain data (Articles 186 through 188).[75] Depending on the

[73] If during a search objects not related to the criminal offence for which a search warrant was issued are found, however, which objects point to the commission of another criminal offence prosecuted ex officio, the said objects shall be described in the minutes and temporarily seized and a seizure receipt shall be immediately issued. The State Attorney shall be immediately notified thereof.
[74] Where the State Attorney establishes that there is no ground for instituting criminal proceedings and where there is no other statutory ground for the seizure of the objects concerned, the said objects shall be immediately returned, of which minutes shall be drafted. The objects used during search of a computer and similar devices shall be returned to their users after the search, provided they are not necessary for the further conduct of criminal proceedings.

circumstances, data that are not related to the criminal offence for which proceedings are undertaken, but which are needed by the person against whom the measure in question has been taken, may be recorded onto an appropriate medium and returned to this person also prior to the conclusion of proceedings."

f) Exceptions to temporary seizure (Article 262 of the CPA)

g) *Limits defined by written reasoned warrant for special evidentiary measures* (Article 335/1 of the CPA)

h) *Data protection rules in the CPA (Article 186) - general application for all CPA measures*

(1) Personal data may be collected by the competent authorities only for purposes specified by law in the framework of their tasks as laid down by the present Act.
(2) Personal data may be processed only in cases specifically provided for by statute or some other regulation and only to such extent as is in line with the purpose for which the data were collected. Further processing of the said data shall be permitted only if it is not incompatible with the purposes for which the data were collected and if the competent authorities are authorised to process such data for such other purpose in accordance with the law and such processing is necessary and proportionate to that other purpose.
(3) Processing of personal data concerning health or sex life shall be permitted only exceptionally if a criminal offence punishable by five years' imprisonment or a more severe penalty could not be detected or proven in any other way or where this would involve disproportionate difficulties.
(4) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership shall not be allowed.
(…)

[75] Article 186: (1) Personal data may be collected by the competent authorities only for purposes specified by law in the framework of their tasks as laid down by the present Act. (2) Personal data may be processed only in cases specifically provided for by statute or some other regulation and only to such extent as is in line with the purpose for which the data were collected. Further processing of the said data shall be permitted only if it is not incompatible with the purposes for which the data were collected and if the competent authorities are authorised to process such data for such other purpose in accordance with the law and such processing is necessary and proportionate to that other purpose. (3) Processing of personal data concerning health or sex life shall be permitted only exceptionally if a criminal offence punishable by five years' imprisonment or a more severe penalty could not be detected or proven in any other way or where this would involve disproportionate difficulties. (4) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership shall not be allowed (...)

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

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

No. Sanctions apply - which do not apply to defendant. Under Article 257 of the CPA, at the request of the authority conducting a search, the person using a computer or having access to a computer or another device or data carrier, as well as a telecommunications service provider shall enable access to a computer, device or data carrier and shall provide the necessary information for unhindered use and achievement of the goals of the search. Where they do not comply, despite there being no justifiable reasons therefore, they may upon the motion of the State Attorney be punished by the judge of investigation (monetary fine up to 50.000,00 Kuna, and if they fail to comply even further, imprisonment until compliance but no longer than one month). Defendant cannot be punished.

No where rules on temporary seizure of computer/mobile phone data under Article 263 of the CPA apply. According to that provision the data must be handed in an integral, original, legible and understandable form. In the case of refusal to hand over data, it may be proceeded in accordance with Article 259, paragraph 1, of the CPA, which means that a monetary fine may be issued against the person up to 50.000,00 Kuna, and if he/she fails to comply even further, he/she may be imprisoned until compliance but no longer than one month. Punishment applies neither to the defendant nor to persons exempted from the duty to testify. The data holder shall be warned of the consequences resulting from non-compliance with the request to hand over the data (Article 261, paragraph 2).

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

No but sanctions apply, which do not apply to defendant. Under Article 257 of the CPA, at the request of the authority conducting a search, the person using a computer or having access to a computer or another device or data carrier, as well as a telecommunications service provider shall enable access to a computer, device or data carrier and shall provide the necessary information for unhindered use and achievement of the goals of the search. Where they do not comply, despite there being no justifiable reasons therefore, they may upon the motion of the State Attorney be punished by the judge of investigation (monetary fine up to 50.000,00 Kuna, and if they fail to comply even further, imprisonment until compliance but no longer than one month.

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

With the serving of the search warrant the *defendant* shall be notified of *his/her rights*, such as on information on what he/she is being charged with and the circumstances giving rise to reasonable grounds for suspicion against him/her (unless he/she had already received the investigation order), the right to inspect the case file (exception – Article 184a of the CPA), that he/she is not obliged to present his/her defense or answer questions, on the right to use their own language and on right to an interpreter, on the right concerning defense counsel (details in Article 239 of the CPA).

Handing of search warrant and prior invitation to voluntarily hand over the device under the CPA: (1) Unless otherwise prescribed by this Act, before a search starts, the search warrant shall be handed to the person whose premises will be searched or who will be searched, or to the person who is in possession of the object of the search. (2) Before the start of the search, the person referred to in paragraph 1 of this Article shall be invited to voluntarily hand over the person or objects searched for (Article 243).

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

Where search is concerned, assumedly yes, but not specified under applicable rules on search under the CPA. There is a prescribed duty to enable access and enable unhindered use/accomplishment of search aims (e.g. passwords, encryption): at the request of the authority conducting a search, the person using a computer or having access to a computer or another device or data carrier, as well as a telecommunications service provider shall enable access to a computer, device or data carrier and shall provide the necessary information for unhindered use and achievement of the goals of the search. Where they do not comply, despite there being no justifiable reasons therefore, they may upon the motion of the State Attorney be punished by the judge of investigation (monetary fine up to 50.000,00 Kuna, and if they fail to comply even further, imprisonment until compliance but no longer than one month). Defendant cannot be punished (Article 257 of the CPA).

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

Where the CPA is concerned only the defendant cannot be sanctioned in case of refusing to comply with the order under Article 257 (search of a movable i.e. mobile device). In cases of refusing to hand over computer data under Article 263 only the defendant and persons exempted from the duty to testify shall not be punished if they refuse to hand over computer data.

25. *What about data stored in the Cloud, what is the procedure to access this data if it is known or suspected to reside outside your jurisdiction? Is international cooperation like the European Investigation Order or Mutual Legal Assistance Treaties the only route or do other options exist? Please elaborate.*

With consent (e.g. provided password) the data may be accessed, otherwise EIO/MLATs are used. According to Ministry of Interior's Report for 2019, during 2018 a total of 209 requests were processed from various organizational units of the police (Ministry of the Interior) for the cross-border acquisition of electronic evidence from various Internet service providers operating outside of the Republic of Croatia.[76]

According to the 2017 Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" – Report on Croatia:

> "In some cases, police officers use the services which some providers of electronic services provide to the police authorities to communicate and to ensure a faster and more effective response to, for example, the exploitation of children for pornography (e.g. Facebook, Skype, and Instagram Law Enforcement Response Team). International police co-operation with the police authorities in some countries (e.g. United States, Australia, New Zealand, etc.) has also been very successful in cases involving sexual abuse and exploitation of children."[77]

Available data on *Government requests for customer data from foreign ISP's* such as Facebook, Google, etc. can be found in *transparency reports* from internet service providers.[78]
Some data is also available in the recent *Cybercrime Convention Committee report: The Budapest Convention on Cybercrime: benefits and impact in practice.*[79]

---

[76] Ministry of the Interior, Report on work for 2019 (title in original language: Izvješće o radu za 2019. godinu), https://mup.gov.hr/UserDocsImages/dokumenti/2019/STUDENI/Godisnje%20izvjesce%20o%20radu%20Ministarstva%20unutarnjih%20poslova.pdf, p. 59.

[77] Council of the European Union, Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime"- Report on Croatia, 5250/1/17, REV 1 DCL 1, GENVAL3 CYBER9, 11.4. 2017, https://data.consilium.europa.eu/doc/document/ST-5250-2017-REV-1-DCL-1/en/pdf, p. 86.

[78] E.g. Facebook: https://govtrequests.facebook.com/about/# Google https://www.google.com/transparencyreport/; Microsoft https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report; Apple http://www.apple.com/privacy/transparency-reports/.

[79] See Requests for account information received/disclosed by Facebook, Google/YouTube and Microsoft/Skype, in: Cybercrime Convention Committee (T-CY), The Budapest Convention on Cybercrime: benefits and impact in practice, T-CY (2020)16, Strasbourg, 13 July 2020, https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac, p. 23.

For more details and suggestions on national contact points for obtaining relevant information on specific practices in this area, please see Section 6 - Comments.

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?*

In cases of applications storing data also on local memory, that is searched and used in procedure. In cases of applications storing data exclusively on online server, seat of server is sought and then international legal assistance mechanisms used. For more details and suggestions on national contact points for obtaining relevant information on specific practices in this area, please see Section 6 - Comments.

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?*

In the context of this questionnaire: if there is no link / application linking to data (in the device), then there is no need to access data in the cloud. Suggestions on national contact points for obtaining relevant information on specific practices in this area are set out in Section 6 - Comments.

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?*

Article 263 of the CPA specifies that the data must be handed over to the State Attorney at his/her written request in an integral, original, legible and understandable form. The State Attorney shall state in his/her request the time limit for the handing over of data. In the case of refusal to hand over data, a monetary fine may be issued against the data holder up to 50.000,00 Kuna, and if they fail to comply even further, they may be imprisoned until compliance but no longer than one month. Punishment does not apply to the defendant and to the persons exempt from the duty to testify.
The police also has the authority to request (seize) data if they carry out this measure in the course of urgent evidentiary actions (Article 212 of the CPA), and where the police carries out a search and finds computer data relating to purpose of the search or data pointing to another criminal offense prosecuted ex officio (Articles 248-249 of the CPA). Data may also be seized by

the police in the scope of their police authority under Article 59 of the Police Duties and Powers Act.[80]

Generally no special warrant shall be necessary for the seizure of data where there is a search warrant. Article 263 of the CPA read in totality provides lack of clarity as to requirement of a prior warrant by judge of investigation (for which action). Namely, according to Article 263 paragraph 5, the person using the computer and the service provider are entitled to file an appeal against the order of the judge of investigation imposing the measure specified in Article 2632, paragraph 3 (which is the recording of data) within the time limit of twenty-four hours. The appeal shall be decided by the panel within the time limit of three days. The appeal shall not stay the execution of the order.

If necessary, for answers on accessing non-content mobile data from operators, see:

a) checking establishment of contact by means of telecommunication for a registered owner/user (Article 339a CPA - only for specific criminal offenses and offences punishable by imprisonment for a term of more than five years); b) verification of contact by electronic communications - Article 68 of the Police Duties and Powers Act (in connection with Article 207 of the CPA on inquiries into criminal offenses) – in Researcher's overview.

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

Due to numerous measures of gathering information that may apply throughout different phases of -proceedings (and even according to different rules) one needs to closely look at each concretely applicable measure in relation to the concrete offense and phase of proceedings. Certain measures can only be applied in respect of certain criminal offenses (see, e.g. Article 332, 339a of the CPA), there are prescribed requirements for the conduct of inquires into criminal offences (if there are grounds for suspicion that a criminal offence prosecuted ex officio was committed - see Article 207 of the CPA), there are prescribed requirements for search and seizure conducted by the police in the scope of urgent evidentiary actions, for criminal offenses that are: 1) punishable by imprisonment for up to five years; 2) punishable by imprisonment of ove five years (see Article 212, paragraph 1 of the CPA), etc.

[80] Petar Veić, Igor Martinović, Izazovi policijskog postupanja u otkrivanju i dokazivanju računalnog kriminala (researcher's translation into English: Challenges of police action in detecting and proving computer crime), Proceedings of the 5th International Scientific and Professional Conference, the Police College Research Days in Zagreb, New Technologies and Methods Used for Improvement of the Police Role in Security Matters, Zagreb, Croatia, 21.-22.4.2016, p. 421.

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

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

Where it is not expressly stated in the CPA that the collected objects/data during pre-trial phases may or may not be used as evidence, there is lack of certainty as to their probative value in court, as it will depend on court practice (e.g. ef officio exclusion, exclusion on the basis of submitted claim). For example, the CPA expressly prescribes that objects seized in violation of Article 262, paragraph 1 of the CPA (prescribing what cannot be seized) cannot be used in evidence in criminal proceedings (Article 262/7). Also, it prescribes that recordings (and documents and objects) obtained by, i.a., interception, collection, and recording of computer data under Article 332 of the CPA (special evidentiary actions temporarily restricting constitutional rights) may be used as evidence in criminal proceedings (Article 333/1). However, where such actions are taken in violation of Article 332 of the CPA, evidence learned from the data thus collected may not be used as evidence in proceedings (Article 335/7). Detailed overview of CPA rules on legality of evidence as well as related case-law is provided in answers to relevant questions (Section 3 - admissibility of evidence before courts). For case law, please see Researcher's overview: "Case law (mobile phone seized)."

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

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

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

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

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

While it would be best practice to specify and record all this (in the protocol on the search/ finding and opinion of expert witness), to my knowledge there are no standard operative procedures nor strict protocol(s) for testing and documenting. Further information should be sought at the Ministry of Interior and/or the State Attorney's Office.

***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?*

None that I am aware of.

***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?*

Please see comments under Section 6.

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

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

Please see comments under Section 6.

***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?*

Please see comments under Section 6.

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

Please see comments under Section 6.

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?*

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

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

Where, for example, during search a mobile phone and/or data was seized, general rules on search such as Article 248, paragraphs 2-3 of the CPA apply, specifying that only such objects and documents that are related to the purpose of a search, as well as objects specified in Article 249, paragraphs 1-2 of of the CPA shall be temporarily seized during the search. The minutes shall describe in detail the objects and documents seized, and this shall be entered in the receipt, a copy of which shall be issued immediately to the person from whom the said objects or documents have been seized.

Under Article 249, if during a search objects not related to the criminal offence for which a search warrant was issued are found, however, which objects point to the commission of another criminal offence prosecuted *ex officio*, the said objects shall be described in the minutes and temporarily seized and a seizure receipt shall be immediately issued. Next, where the State Attorney establishes that there is no ground for instituting criminal proceedings and where there is no other statutory ground for the seizure of the objects concerned, the said objects shall be immediately returned, of which minutes shall be drafted.

The objects used during search of a computer and similar devices shall be returned to their users after the search, provided they are not necessary for the further conduct of criminal proceedings.

Personal data obtained by a search may only be used for the purposes of criminal proceedings and shall be erased without delay when this purpose ceases to exist.

Rules on temporary seizure of objects (Aricles 261-270) specify which objects, including data (Article 263 – data stored in computers and devices connected thereto, as well as in devices used for collecting and transferring data, data carriers, subscription information in the possession of a service provider) can and cannot be seized and/or be withheld, details on content of minutes as regards temporarily seized objects/data and on receipt of a temporarily seized object, the keeping of seized objects, etc.

The provision specifically applying to analysis and management of data from mobile devices would be Article 263 of the CPA, according to which rules on temporary seizure (Article 261) also apply to data stored in computers and devices connected thereto, as well as in devices used for collecting and transferring data, data carriers and subscription information in the possession of a service provider (except in cases where temporary seizure of objects is prohibited under Article 262 of this Act).

According to Article 263, who holds such data must hand them over to the State Attorney at his/her written request in an integral, original, legible and understandable form. The State Attorney shall state in his/her request the time limit for the handing over of data. In the case of refusal to hand over data, it may be proceeded in line with Article 259, paragraph 1. That provision specifies that a monetary fine shall be issued against the person up to 50.000,00 Kuna, and if he/she fails to comply even further, he/she shall be imprisoned until compliance but no longer than one month. Punishment does not apply to the defendant and persons exempt from the duty to testify.

The data shall be recorded in real time by the authority taking the action.

In acquiring, recording, protecting and storing of data special attention shall be paid to rules on the confidentiality of certain data (Articles 186 through 188[81]).

Depending on the circumstances, data that are not related to the criminal offence for which proceedings are undertaken, but which are needed by the person against whom the measure in question has been taken, may be recorded onto an appropriate medium and returned to this person also prior to the conclusion of proceedings.

Upon a motion of the State Attorney, the judge of investigation may decide by an order that all mentioned computer data be preserved and safeguarded for as long as necessary, but not exceeding a period of six months. Afterwards the computer data shall be returned unless:

1) they concern the commission of criminal offences against computer systems, programmes and data (Title XXV) of the Criminal Code;
2) they are related to the commission of another criminal offence prosecuted ex officio, which was committed by means of a computer system;
3) they are to be used as evidence of a criminal offence for which proceedings are ongoing.

[81] Article 186: (1) Personal data may be collected by the competent authorities only for purposes specified by law in the framework of their tasks as laid down by the present Act. (2) Personal data may be processed only in cases specifically provided for by statute or some other regulation and only to such extent as is in line with the purpose for which the data were collected. Further processing of the said data shall be permitted only if it is not incompatible with the purposes for which the data were collected and if the competent authorities are authorised to process such data for such other purpose in accordance with the law and such processing is necessary and proportionate to that other purpose. (3) Processing of personal data concerning health or sex life shall be permitted only exceptionally if a criminal offence punishable by five years' imprisonment or a more severe penalty could not be detected or proven in any other way or where this would involve disproportionate difficulties. (4) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership shall not be allowed (...). *For other provisions please see Researcher's overview.*

The person using the computer and the service provider are entitled to file an appeal against the order of the judge of investigation imposing the measure (recording the data, i.e., measure specified in Article 2632, paragraph 3) within the time limit of twenty-four hours. The appeal shall be decided by the panel within the time limit of three days. The appeal shall not stay the execution of the order.

According to the Report on Croatia for the Council of the EU in relation to fight against cybercrime[82], in connection with the data obtained under Article 263 of the CPA "the complete recording and documentation shall be sealed and kept in the State Attorney's Office", *in line with Article 338, paragraph 2 of the CPA* (see below). That provision, as enacted in the CPA, falls under the relevant section on special evidentiary measures in Article 332. While, logically, the stated measure (Article 338/2) should apply *per analogiam* also in cases of seizure of computer data specified in Article 263, fact is that currently no CPA provisions are explicitly and specifically designated for the cases of computer data seizure. See also provisions of Articles 267, 269 and 270 of the CPA.

Article 338
(1) The recordings, documents and objects obtained through the actions referred to in Article 332, paragraph 1, of this Act may be used in evidence only in proceedings against the person referred to in Article 332, paragraph 1, of this Act or in the case referred to in Article 335, paragraph 6, of this Act.
(2) Recordings, transcripts and documentation shall be kept sealed in the State Attorney's Office in their entirety. Where circumstances allow, the judge of investigation shall order, upon the motion of the State Attorney, that only those parts of a recording, transcript and documentation which refer to the criminal proceeding in question be included in the case file.
(3) For this purpose the State Attorney shall serve on the judge of investigation a motion which includes a statement of reasons and the full version of the recording which the judge of investigation shall return after the part of the recording which refers to the criminal proceedings in question is singled out. The singling out shall be made by an expert assistant under the supervision of the judge of investigation.
(4) The State Attorney shall enable the defendant immediately upon his request to reproduce a recording or inspect a transcript or documents. After the recording has been reproduced or the transcript or documents inspected, the defendant may propose at the trial that the recording, transcript or documents be reproduced or read out in full or in part."

Collecting and presenting documentary evidence (Article 329; Articles 267 and 269)

[82] Council of the European Union, Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime"- Report on Croatia, 5250/1/17, REV 1 DCL 1, GENVAL3 CYBER9, 11.4. 2017, https://data.consilium.europa.eu/doc/document/ST-5250-2017-REV-1-DCL-1/en/pdf, p. 51.

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

(1) Documents that serve to establish facts shall be obtained and kept in application of the provisions of this Title**,** taking care not to damage or destroy any document and to preserve its contents in unmodified form. Where necessary, the authority conducting the proceedings shall, after having verified the document accordingly, make a copy of it and return the original to the person who submitted the document.
(2) With regard to documents, it shall be proceeded as with other objects that are to be used in evidence (Articles 267 and 269).
(3) Documentary evidence shall be presented by way of its reading or examination .

Collecting and presenting recording evidence (Article 330; Articles 267 and 269)

(1) A recording serving to establish facts shall be obtained in application of the provisions of this Title.
(2) With regard to a recording, it shall be proceeded as with other objects that are to be used in evidence (Articles 267 and 269), taking care not to damage or destroy the recording and to preserve its contents in unmodified form. Where necessary, appropriate measures shall be taken in order to preserve the recording in unmodified form or to make a copy of it.
(3) Unless otherwise prescribed by this Act, the contents of a recording shall be established by reproduction. If the recording includes footage of a child, the recording shall be reproduced by modifying the image and the voice of the child where this is required for the purpose of protecting the interests of the child. In doing so, account shall be taken of the interests of the proceedings as a whole.
(4) A recording shall be reproduced by an expert.

Managing seized objects (files, documents,objects)

Article 267
(1) The files or documents which have been temporarily seized because they may be used in evidence shall be listed. Where this is not possible, the files or documents shall be placed in an envelope and sealed. The person from whom a file or document is temporarily seized may place his/her seal and signature on the envelope.
(2) The envelope shall be opened by the State Attorney. *While examining files or documents, care must be taken not to disclose their contents to unauthorised persons*. *A protocol of the opening of the envelope shall be made*.
(3) The person from whom the files or documents have been seized shall be summoned to be present at the opening of the envelope. If the said person does not respond to the summons or is absent, the envelope shall be opened, the files or documents examined and an inventory of them made in his absence.

Article 269
(1) Before the indictment is preferred, objects that are to serve as evidence shall be kept in a special room of the State Attorney's Office. Afterwards they shall be kept in a special room at the court building. By way of exception, where this is not possible, these objects shall be kept off the State Attorney's or court premises.
(2) The authority conducting proceedings shall be in charge of supervising these objects.
(3) The minister responsible for justice shall adopt regulations on the method of and conditions for the safekeeping of objects referred to in paragraph 1 of this Article. [83]

Article 270
(1) Temporarily seized objects shall be returned as soon as they are no longer necessary for the further conduct of the proceeding unless under the law they are subject to the provisions on seizure or where statutory reasons for applying the measure referred to in Article 266, paragraph 2, of this Act cease to exist.(2) The State Attorney and the court shall, ex officio, take care that the reasons for keeping temporarily seized objects have not ceased to exist.

Rights of the defendant and injured person regarding the protocol[84] (e.g. protocol on the taking of evidentiary action such as search of a mobile phone): reading the protocol, placing objections.[85]

[83] The *Ordinance on the handling of found and seized objects* (title in original language: Pravilnik o postupanju s pronađenim i oduzetim predmetima, Official Gazette no. 50/2012, regulates the manner and conditions under which found or confiscated items are kept, which may serve in establishing the facts in criminal proceedings or as evidence until the indictment is filed ("Corpore delicti"). According to Article 11, at the request of the State Attorney, data stored in computers and devices connected thereto, as well as in devices used for collecting and transferring data, must be handed over to the State Attorney, in accordance with the CPA. If, at the proposal of the State Attorney, the judge of investigation orders the protection and storage of computer data that have been temporarily seized, these data shall be kept in Corpora delicti for a maximum of six months, after which the computer data must be returned, unless otherwise provided by the CPA.

[84] Article 82 of the CPA: (1) A protocol shall be drawn up about every action taken in the course of proceedings concurrently with the action's taking and where this is not possible, immediately afterwards. (2) The protocol shall be drawn up by the recorder. Only in cases of search of a home or of a person or where an action is taken outside the authority's official premises and the recorder is not available may the protocol be drawn up by the person taking the action in question. (3) Where the protocol is drawn up by the recorder, it shall be drawn up in such a manner that the person taking the action dictates to the recorder what he/she is to enter in the protocol. (4) The person being interrogated may be permitted to state answers directly on the protocol. In the case of abuse the said person may be denied this right. Article 83 of the CPA: (1) The protocol shall contain the name of the government authority before which an action is taken, the location at which the said action is taken, the date and exact time when the action in question commences and ends, the names of the persons present, including in what capacity they are present, and the identification marking of the criminal case in which the action is taken. (2) The protocol must contain essential information on the course and contents of the action taken. Only the essential contents of statements and declarations

In the scope of the Judicial Academy in December 2016 the personnel at the County State's Attorney Office created training materials on *IT expertise in criminal proceedings* (researcher's translation into English)*:*

> "The main problems that arise when conducting these evidentiary actions are primarily the recognition of electronic evidence, given its nature, i.e. the fact that it is often invisible, and there is a danger that this evidence can be easily erased, altered, damaged or manipulated, and during further course of proceedings it is necessary to establish and confirm its authenticity. Also, given the variability of electronic evidence, it must be secured in such a way that it must be available for a longer period of time. Given all these circumstances, taking electronic evidence is particularly sensitive and that is why a guide called "Taking e-evidence"[86] has been adopted. This guide sets out general principles for the handling of electronic evidence, with the key issues being how to ensure the legality of the proceedings and to ensure the integrity of the proceedings with the help of experts and trained officials, in order to ensure the legality."[87]

However, there are no further details and/or reference on the mentioned guide itself in this training material.[88]

---

made shall be entered in the protocol in the narrative form. Questions shall be recorded in the protocol only where this is necessary for understanding the answers. Where necessary, the question asked and the answer given to it shall be entered in the protocol verbatim. If objects and documents are seized in the course of taking an action, this shall be recorded in the protocol and the seized objects shall either be attached to the protocol or their location shall be stated. (3) When taking actions such as inspection, search, temporary seizure of objects or identification, information that is important in view of the significance of such an action or for determining the identity of certain objects (description, measures and size of objects or traces, marking of objects, etc.) shall also be entered in the protocol. Where sketches, drawings, blueprints, photographs, film or other technical recordings are made, this shall also be stated in the protocol and attached to it. (4) Special provisions on the protocol shall apply to the trial protocol (Articles 409 through 412), deliberation and voting protocols (Article 88) and other protocols as prescribed by this Act. Article 84 of the CPA: (1) The protocol shall be taken in an orderly manner. There may be no additions or changes to it. The parts crossed out must remain legible. (2) All changes, corrections and additions shall be entered at the end of the protocol and shall be certified by the persons signing the protocol.

[85] Article 85 of the CPA: (1) The person interrogated, the persons whose presence during the taking of actions in the proceedings is mandatory and, if present, the parties, defence counsel and injured person shall be entitled to read the protocol or request that it be read to them. The person taking the action shall inform them of this right. A note shall be entered in the protocol as to whether this information was given to the persons in question as well as whether the protocol was read. The protocol shall always be read if no recorder is present and a note thereon shall be entered in the protocol. (…) (7) If objections are raised concerning the contents of the protocol, these objections shall be noted in the protocol as well.

[86] Title in original language is: "Uzimanje e-dokaza".

[87] Judicial Academy, Križanić, Gordana (County State Attorney's Office in Karlovac), Expertise in criminal proceedings: IT expertise (title in original language: Vještačenje u kaznenom postupku - informatičko vještačenje), December 2016, http://pak.hr/cke/obrazovni%20materijali/Vje%C5%A1ta%C4%8Denje%20u%20kaznenom%20postupku.pdf, p. 30.

[88] Possibly it is the Council of Europe's Electronic Evidence Guide? For accuracy and further details I advise contacting the relevant author / State Attorney's Office.

Mentioned training materials (December 2016) from the State Attorney's Office conclude that IT experts are rarely used, and if expertise is used, it is as a rule telecommunications expertise.

> "As a rule, when we have seized computers or mobile phones at our disposal, we decide on the evidentiary action of the search and our decision on the merits is based on the minutes of the search. The question here is whether it is enough to be satisfied with this evidentiary action, or whether it would be much more correct to order an IT expertise. There is also the question of contamination of evidence, and consequently the question of illegality of evidence that is the result of unprofessional handling during the seizure of material." [89]

Information on available training/education (up to 2017) in the wider scope of preventing and combatting cybercrime, including training on digital evidence forensics, is available at the Evaluation report on Croatia in the scope of "The practical implementation and operation of European policies on prevention and combating cybercrime" (Council of the European Union).[90]

In domestic literature (2016) there are examples of practices used in the seizing of computers / mobile phones / digital trace holders:

> "If computers or other electronic trace media to be seized are found during the search, the home screen on the device will be photographed (if the device is turned on), after which the device will be turned off and packaged in a way that the entire computer will be lined with paper, foil or in another way and sealed with an official seal in order to prevent the opening of the computer without removing the seal, and thus ensure the so-called unbroken chain of evidence, after which the computer is taken to the official premises of the police. The only difference is in the handling of mobile and similar devices, when the device will not be turned off (due to the possibility of password protection), but will be packed while turned on. Seizure of the computer or other electronic trace holder will be stated in the minutes of the search and a receipt on temporary seizure of items to the person undergoing the search, and if the computer or other holder of electronic traces is seized without a search, then in addition to the receipt on temporary seizure of items also minutes on temporary seizure of items will be made (no warrant). In this way, all formal conditions regarding the procedure of seizing the computer / digital trace holders have been met, and it will be possible to use them as evidence in possible court proceedings."

---

[89] Judicial Academy, Križanić, Gordana (County State Attorney's Office in Karlovac), Expertise in criminal proceedings: IT expertise (title in original language: Vještačenje u kaznenom postupku - informatičko vještačenje), December 2016, http://pak.hr/cke/obrazovni%20materijali/Vje%C5%A1ta%C4%8Denje%20u%20kaznenom%20postupku.pdf, p. 33.

[90] Council of the EU, Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime"- Report on Croatia, 5250/1/17, REV 1 DCL 1, GENVAL3 CYBER9, 11.4. 2017, https://data.consilium.europa.eu/doc/document/ST-5250-2017-REV-1-DCL-1/en/pdf, pp. 92-97.

The same author considered it extremely useful to have a standard operative procedure with steps to be taken when seizing the computer at the Ministry of the Interior. In regard to the *subsequent process of search* (forensic investigation), the author stated:

> "In the organizational unit of the police that initiated the entire procedure, the procedure is taken over by a police officer who has the highest level of knowledge of computer technology, although he/she does not necessarily have to be educated for that. Namely, in the system of the Ministry of the Interior there is no special program for training police officers in this area, but it all comes down to personal experience and knowledge of police officers, based on which the immediate superior should determine the competencies of the police officer.
> These indicators have resulted in each computer forensic investigator using different programs in their work and there is no prescribed standardization regarding software solutions in the processing of digital traces in the Republic of Croatia. This actually means that any computer forensic investigator can use any digital trace processing program, so although there are no written results of this mode of operation, it would be very interesting to see if the use of other, free forensic tools has effects on the efficiency and quality of the conduct of the evidentiary action of search of a movable by police investigators, but also on the level of credibility of such traces in the later stages of criminal proceedings."[91]

According to the recently published news at the website of the Ministry of the Interior beginning of 2020, the project "Strengthening the capacity of the Ministry of the Interior in the fight against all forms of cybercrime" will enable procurement of necessary software and fardware as well as training on digital evidence and forensic methods and procedures for 31 police officers:

> "As part of the project, the necessary equipment and computer programs will be procured that will enable the efficient execution of court orders for the search of electronic evidence holders. The Independent Sector for Schengen Coordination and European Union Funds of the Ministry of the Interior has decided to allocate financial resources for the implementation of the project: "Strengthening the capacity of the Ministry of the Interior in the fight against all forms of cybercrime." (….)
> The project consists of two components:
> 1. Equipping the organizational units of the Ministry of the Interior with the necessary software and hardware components
> 2. Implementation of educational modules on digital evidence and forensic methods and procedures for 31 police officers
> The project will procure the necessary equipment and computer programs that will enable the efficient execution of court orders to search electronic evidence carriers such as computers, tablets, hard disks and mobile phones. The aim of the training is to raise the competencies of police officers for the successful suppression of cybercrime. The training includes the following topics: Basics of attack and

[91] Nikola Protrka, Krešimir Filipić, Uloga forenzičkog softvera EnCase pri radu s elektroničkim tragovima (The role of forensic software EnCase with digital trace), Kriminalistička teorija i praksa, Vol. 3. No. 2/2016., 2016., pp. 121-134, at pp. 125-127. Note: text translated into English by researcher.

protection of information systems and information security; Information technology architecture, models, mechanisms and principles; Digital traces, evidence and forensics, and Prevention, surveillance and specialized areas of cyber attacks (...)".[92]

According to the Police Duties and Powers Act, an investigator may be a police officer who has at least five years of work experience in the field of crime prevention, and the investigator who examines a witness or a defendant may be a police officer with at least the personal police rank of police sergeant. Both types of investigators must have special knowledge and must be specially trained. Programs of additional professional training for investigators shall be adopted by decision of the Minister of the Interior, with prior opinion of the Chief State Attorney (Article 11b). Investigators are appointed by the Director General of the Police with the previously obtained opinion of the Chief State Attorney (Article 11 c).

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?*

Already discussed above, additionally: none that I am aware of.

***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.*

General rules on inadmissibility of evidence apply. Constitution of Republic of Croatia prescribes that evidence obtained unlawfully may not be admitted in court proceedings (Article 29, paragraph 4).
Under Article 10, paragraph 1 of the Criminal Procedure Act, court decisions may not be founded on unlawfully obtained evidence (unlawful evidence), and that is evidence (Article 10, paragraph 2):
1) obtained in violation of the prohibition of torture, inhumane or degrading treatment provided for in the Constitution, statute or international law;
2) obtained in violation of the rights to defence, dignity, reputation and honour, and the rights to inviolability of personal and family life guaranteed by the Constitution, domestic or international

[92] Ministry of the Interior, https://mup.gov.hr/vijesti/aktivnosti-u-sklopu-projekta-jacanje-kapaciteta-mup-a-u-borbi-protiv-svih-oblika-kibernetickog-kriminaliteta/285974, 08.1.2020. Translated into English by researcher.

law, except if such evidence was obtained in proceedings for grave forms of criminal offences falling within the jurisdiction of the county court[93] and with respect to which the interest of the perpetrator's criminal prosecution and punishment prevails over the violation of a right – however, in such cases the court decision may not be founded exclusively on such evidence (Article 10, paragraph 4 in connection with Article 10, paragraph 3 and Article 10, paragraph 2, item 2 of the CPA)
3) obtained in violation of criminal procedure provisions which is expressly provided for in the Criminal Procedure Act (unlawful evidence ex lege);
4) of which knowledge has been gained from unlawful evidence ("fruit of the poisonous tree").

Electronic (digital) evidence is defined in Article 202, paragraph 2, point 33 of the CPA as data, which was obtained as evidence in electronic (digital) form under this Act. Unless prescribed otherwise in the CPA, electronic evidence is obtained (collected) by applying provisions of Articles 257 on search of a movable, and provisions of Articles 262 and 263 on the temporary seizure of objects (Article 331).

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?*

It depends on what procedural rules were not followed (please see relevant provisions and detailed case law according to different scenarios in Researcher's overview). Namely, under Article 10 of the CPA ex lege unlawful evidence is evidence obtained in violation of criminal procedure provisions which is expressly provided for in the CPA (e.g. violations of search rules as specified in Article 250; violations of Article 332 - per Article 335, paragraph 7 of the CPA; violations of rules on excluded objects for seizure - Article 262, paragraph 1 as per Article 262, paragraph 7; Article 263, paragraph 1 of the CPA; (unlawful) finding and opinion of a person who may not be appointed as expert witness (Article 311, paragraph 1 of the CPA). Also, it is evidence of which knowledge has been gained from unlawful evidence (e.g. minutes on search of the mobile phone represents unlawful evidence, where it became known from the unlawfully seized mobile phone, which may not be used as evidence in the proceedings - contravention of Article 250 of CPA, or, when object (mobile device / data) were seized in violation of Article 262, paragraph 1 (as per Article 262, paragraph 7; Article 263, paragraph 1 of the CPA). Shortcoming such as that minutes on seizure of a movable did not contain a note where the object

[93] See Article 21 of the Act on the Office for the Supression of Corruption and Organized Crime (USKOK).

was found (as prescribed by Article 262, paragraph 6 of the CPA[94]) did not in case law by itself render such evidentiary action unlawful.[95] Also, acting contrary to Article 257, paragraph 2 of the CPA by not taking measures to prevent data destruction/ modification during search would not make evidence obtained unlawful *per se*[96], neither would the shortcomings/lacking in reasoning in the search warrant (not specified in Article 250 of the CPA). [97]

Under Article 10 of the CPA court decisions may also not be founded on evidence obtained in violation of the rights to defence, dignity, reputation and honour, and the rights to inviolability of personal and family life guaranteed by the Constitution, domestic or international law, *except if such evidence was obtained in proceedings for grave forms of criminal offences falling within the jurisdiction of the county court*[98] *and with respect to which the interest of the perpetrator's criminal prosecution and punishment prevails over the violation of a right* – however, in such cases the court decision may not be founded exclusively on such evidence (Article 10, paragraph 4 in connection with Article 10, paragraph 3 and Article 10, paragraph 2, item 2 of the CPA).

In case law relating to evidence being a recording that was made without the order of the judge of investigation and without the knowledge and approval of the accused, there is recognition of mentioned exception. The Supreme Court in capacity of apellate court amended the decision of the court of first instance, which decided that the recorded conversation on a dictaphone (with dictaphone) with the defendant (accused for the criminal offense of bribing representatives), which recording was made without the order of the judge of investigation and without the knowledge and approval of the accused, should be excluded as unlawful evidence (Article 10, paragraph 2, item 2 of the CPA) as well as other evidence created by listening to a digital recording of the conversation recorded (fruit of the (“fruit of the poisonous tree” - Article 10, paragraph 2, item 4 of the CPA). The Supreme Court held that such evidence is nonetheless lawful, since it was obtained in proceedings for grave forms of criminal offences falling within the jurisdiction of the county court and with respect to which the interest of the perpetrator's criminal prosecution and punishment prevails over the violation of his (privacy) right (Article 10, paragraph 2, item 2 of the CPA). This is taking into account circumstances of the specific case, and especially having in mind the interest of the entire Croatian society and the prevention of the so-called "trade in mandates."[99] More recently, the Supreme Court affirmed the lower court’s

[94] ”Upon seizing an object, it shall be noted in the minutes where the object in question was found, the object shall be described and, where necessary, the establishment of its identity shall also be ensured in some other way. A receipt shall be issued for temporarily seized objects.”
[95] Supreme Court of the Republic of Croatia, decision, I Kž 658/15-4, 12.1.2016.
[96] Supreme Court of Republic of Croatia, Kžm 25/2019-4, decision, 05.9.2019.
[97] E.g.: Constitutional Court, U-III-4567/2017, 07.2.2018; Supreme Court of Republic of Croatia, I Kž-191/16-5, 13.4.2016. In the concrete case, the juge of investigations issued the warrant on the basis of (referencing to) a reasoned request, in detail, by the State's Attorney.
[98] See Article 21 of the Act on the Office for the Supression of Corruption and Organized Crime (USKOK).
[99] Supreme Court of Republic of Croatia, decision, I Kž-Us 6/14-4, 21.1.2014.

decision allowing as evidence the audio recording of the defendant, obtained without his knowledge, taking into account that the defendant was in capacity of a surgeon accused for the criminal offense of taking a bribe[100] and that the interest of his criminal prosecution and punishment prevail over the violation of his rights.[101]

***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?*

In my opinion, if access to such data was enabled (usernames, passwords, etc.) / provided voluntarily (which consent was documented and established in proceedings, and with any other applicable procedural requirements specifically to the case at hand are observed), such evidence would be admissible (and if such evidence is available in form of a local copy, it will be admissible if obtained by lawful search). Please see also additional information and suggestions on national contact points in Section 6.

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

In order for the evidence to be illegal in the sense of Art. 10, paragraph 2, item 3, of the CPA, it must be obtained in violation of the provisions of criminal procedure and its illegality expressly provided by law. In my opinion this scenario would be assessed by the court more in terms of reliability / credibility of evidence than in terms of its admissibility (for admissibility, see e.g. prescribed circumstances affecting admissibility of evidence obtained by search, as well as minutes/protocol of the search specified in Article 250 of the CPA). Minutes/protocol of the

[100] I.e. a grave form of criminal offences falling within the jurisdiction of the county court (Article 21 of the Act on the Office for the Supression of Corruption and Organized Crime – USKOK).
[101] Supreme Court of Republic of Croatia, decision, I Kž-Us 28/2020-4, 09.4.2020.

search should note such circumstances and where necessary explanations and clarifications provided by expert witnesses.

According to case law, which could apply per analogiam to (modern) mobile devices, claims of alleged manipulation of electronic evidence obtained by search did not affect the issue of admissibility of obtained evidence. Namely, the Supreme Court affirmed the lower court's decision denying the defendant's request to exclude from files as evidence minutes on search of a movable (laptop) together with related evidence. The defendant claimed that the police did not take measures to prevent the destruction or modification of data in her computer, which was seized and searched some time after she was arrested, so that the data could have been manipulated when the computer was out of her reach (alleged contravention of Article 257, paragraph 2 of the CPA[102]). Besides such claim not being backed up by any argumentation, the Supreme Court found that such claim would not affect the legality of conducted search under Article 257 (once the laptop was temporarily seized, and searched the next day under the warrant and with presence of the defense counsel) and of evidence thus obtained (minutes of the search). According to the Court, acting contrary to Art. 257, paragraph 2 of the CPA does not make the action or evidence obtained by the search illegal, because the same is not prescribed in Article 250 of the CPA. In order for the evidence to be illegal (in the sense of Art. 10, paragraph 2, item 3, of the CPA), it must be obtained in violation of the provisions of criminal procedure and its illegality expressly provided by law. Any defendant's claim on potential manipulation may only be examined from the point of view of reliability, which is possible in the further phase of the proceedings.[103]

In another case (also possible application *per analogiam* to mobile devices) the Supreme Court denied the request of the accused person for extraordinary review of final judgment, and according to this decision, claims on lack of reliability of evidence were discussed before the first and second instance court and expert examination was conducted, during which disputable issues were clarified:

> "… the accused unsuccessfully complains about the legality of the search of the laptop […], stating that the laptop was not only the subject of the search but at the same time a means for the otherwise illegal search of the SD card, because the contents of that card were viewed on the laptop in question. This information, connected with an extremely unprofessional search of the laptop (which the applicant corroborates by claiming that no so-called backup was made on the computer before opening the files in the computer) resulted in the fact that during the expert examination it was no longer possible to determine whether files were opened [at a specific time period], including those that are the subject of the incrimination, which made it impossible to verify the authenticity of the testimony of witness. The

[102] Upon the order of the authority carrying out a search, the person using a computer or having access to a computer and other devices referred to in paragraph 1 of this Article, and a telecommunications service provider, shall immediately take measures to prevent the destruction or modification of data. The authority carrying out a search may order that an expert assistant take these measures.
[103] Supreme Court of Republic of Croatia, Kžm 25/2019-4, decision, 05.9.2019.

accused himself added that memory cards were inspected on his laptop which were found in the bag, instead of on another computer, which enabled the transfer of files from memory cards to the computer and vice versa, which means that after that neither the computer nor memory cards could be credible evidence due to suspicion of their contamination."

The Court confirmed the findings of both the first and second instance court, that the laptop was searched on the basis of a previously issued search warrant, so the defense's motion to separate the evidence as unlawful was properly rejected.

"The fact that on the same occasion, when the computer was searched, the SD memory card was searched on the same computer, for the search of which no warrant of the investigating judge was issued, so that part of the search record was separated as unlawful (by first and second instance court decisions), does not make the computer search illegal. These are two searches that each form a separate unit, and the fact that one protocol (minutes) was made of both did not result in a different qualification of these actions as separate evidence. Finally, illegality of the search of the SD memory card led to the exclusion of the part of search minutes related to search of that card. The question, however, whether and to what extent the search of the SD memory card for which no warrant was issued by the investigating judge, could "contaminate" with its content the computer for which the warrant existed, is possibly an objection to the credibility of evidence, *i.e.*, minutes of the computer search, which is essentially a question of fact, and on what grounds the filing of this extraordinary remedy is not permitted. Of the same meaning is the "unprofessional" way of conducting a computer search, which is explained in detail by the accused, i.e., the consequent inability to determine the earlier dates of access to individual files. The first-instance and second-instance courts commented on these allegations of the accused, which actually warn of certain shortcomings and shortcomings of the probative value of conducted search, after an expert examination was conducted, during which all disputable issues were clarified, since that is also a matter of objection on credibility of evidence, and not its lawfulness."

As regards the SD card, the Court noted that although it was searched unlawfully the first time, the card was searched subsequently upon the issued warrant and thus such latter search thereof was lawful: "the fact that content of the mentioned memory card was determined for the first time on the basis of an illegal search did not result in the illegality of the holder of that content - the SD memory card itself." [104]

***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.*

[104] Supreme Court of Republic of Croatia, judgment, III Kr 165/11-5, 19.9.2012.

Not to my knowledge. The protocol (minutes) should contain the means, methods and sotware/hardware used.

***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.*

The Supreme Court of the Republic of Croatia, as a court of second instance, affirmed the lower court's decision denying the objection on illegality of measures for monitoring SMS messages and recordings of telephone conversations due to the fact that audio recordings are heard on recordings even before contacts of monitored telephone numbers were made. Special evidentiary action of secret surveillance of communication also implies the surveillance of communication by SMS messages sent via monitored numbers from these telephones, and the issue of minor difficulties regarding the implementation technique itself, i.e., the circumstance that the recording starts a few moments before telephone connections are established, does not constitute this evidence illegal.[105]

In domestic case law defendants filed appeals to decisions of courts refusing to exclude evidence as unlawful where scope of the measure appeared to be excessive. For example, the defendant claimed that during the secret surveillance and technical recording of telephone conversations and other remote communications more data was recorded, i.e., also the data preceding the establishment of a telephone call or which occured after the end of a telephone conversation, and which had nothing to do with that conversation. According to the court, technical recording of telephone conversations, by its nature, stipulates that the recording starts from the establishment of a telephone connection between the caller and called party, which means that it is not allowed to record any sound before establishing such contact, because this would entail another measure (technical recording of persons). Therefore, in order to assess the merits of the appellant's complaint that the recording was made unlawfully because the conversation was recorded through the microphone of the mobile phone even before a particular call was made, it was necessary to state in the minutes what was heard by listening to the audio recordings, and, if established that such recordings also contained such data, extract (exclude, separate) those parts of the recordings. Where only incomprehensible tones were heard before the connection was established, then no exclusion would be necessary, if such noises are not relevant in the procedure.[106]

[105] Supreme Court, decision, I Kž 658/14-7, 20.5.2015.
[106] Supreme Court, I Kž 549/11-4, 31.8.2011.

***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.*

Not to my knowledge. Please see detailed answer to question 37.

***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?*

Under Article 10 of the Criminal Procedure Act, court decisions may not be founded on unlawfully obtained evidence (unlawful evidence), and that is also evidence obtained in violation of the rights to defence, dignity, reputation and honour, and the rights to inviolability of personal and family life guaranteed by the Constitution, domestic or international law, *except if such evidence was obtained in proceedings for grave forms of criminal offences falling within the jurisdiction of the county court*[107] *and with respect to which the interest of the perpetrator's criminal prosecution and punishment prevails over the violation of a right – however, in such cases the court decision may not be founded exclusively on such evidence* (Article 10, paragraph 4 in connection with Article 10, paragraph 3 and Article 10, paragraph 2, item 2 of the CPA).
According to accepted court practice, recordings made by another person without authorization and without knowledge of the recorded person cannot be used in the evidentiary procedure because they are illegal evidence in the sense of Article 10, paragraph 2, item 2 of the CPA due to violation of that person's rights to privacy and inviolability of personal life. Thus, for example, a court decision cannot be based on private video and audio recordings of the defendant, made by the injured party with her/his mobile phone, even though they were voluntarily submitted by that injured party (on which the procedural forms of the CPA on how to obtain evidence lawfully do not apply, but only on state bodies), in cases where such such recording was procured in violation of the Criminal Code[108], i.e., where the defendant had not been aware of such recording / had not

[107] See Article 21 of the Act on the Office for the Supression of Corruption and Organized Crime (USKOK).
[108] In violation of Article 143 (Unauthorised Audio Recording and Eavesdropping) or Article144 (Unauthorised Taking of Pictures). County Court in Zagreb, decision, 9 Kž-438/2017-3, 11.7.2017.

agreed to be recorded.[109] It is not relevant where the conversation was taking place (whether in private or public space).[110]

***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.*

Minutes on search of the mobile phone represents unlawful evidence, where it became known from the unlawfully seized mobile phone, which may not be used as evidence in the proceedings. In the concrete case the mobile phone, as evidence which may be used in criminal proceedings, was seized by the police in the defendant's home without consent of the defendant, which "search" was conducted without a warrant of the defendant's home in contravention of the Criminal Procedure Act. Such unlawfulness is not remedied by the fact that defendant as mobile phone owner was "cooperative" in the police station, after his mobile phone had already been unlawfully seized by the police, and that he himself opened the mobile phone and took out SIM cards. [111]

In relation to formal requirements of the warrant for special evidentiary measures – secret telecommunication surveillance under the CPA, the European Court of Human Rights rendered several judgments against Croatia on violation of Article 8 of the European Convention on Human Rights. According to the Court such warrants did not provide adequate reasoning as to particular circumstances of the case and in particular reasons why the investigation (*inquiries into criminal offenses*) could not be conducted by other, less intrusive, means. [112] „The Supreme Court of the Republic of Croatia accepted such a position of the European Court of Human Rights and revised its previous position, in such a way that in a situation when the order for special evidentiary actions temporarily restricting certain constitutional rights of citizens has no legally prescribed reasoning, evidence obtained on the basis of such of a deficient reasoned order are illegal evidence, cannot be justified by subsequent judicial control and must be separated from

[109] Supreme Court of Republic of Croatia, III Kr 11/17-5, 22.2.2017.
[110] County Court in Zagreb, decision, 9 Kž-438/2017-3, 11.7.2017.
[111] Supreme Court of the Republic of Croatia, decision, I Kž 658/15-4, 12.1.2016.
[112] Dragojević v. Croatia, no. 68955/11; Bašić v. Croatia, no. 22251/13, Matanović v Croatia, no. 2742/12; Grba v. Croatia, no. 47074/12, Parazajder v. Croatia, no. 50049/12; Bosak and others v. Croatia, nos. 40429/14 and 3 others .

the case file, unless the preconditions from Art. 10 paragraph 3 of the CPA / 08 have been met." [113]

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?*

Electronic (digital) evidence is defined in Article 202, paragraph 2, point 33 of the CPA as data, which was obtained as evidence in electronic (digital) form under this Act. Unless prescribed otherwise in the CPA, electronic evidence is obtained (collected) by applying provisions of Articles 257 on search of a movable, and provisions of Articles 262 and 263 on the temporary seizure of objects (Article 331). Under Article 430 of the CPA, unless prescribed otherwise in this Act, evidence obtained by examining documents or reproducing recordings and electronic evidence shall be presented before the Court as set forth in Articles 329 through 331 of this Act (provisions are laid out in Researcher's overview).

[113] Supreme Court of Republic of Croatia, judgment, I Kž-Us 7/2018-6, 13.2.2020. Additionally: I Kž-Us 26/17.-5, 04.5.2017; I Kž-Us 26/17.-5, 05.9.2017; I Kž-Us 165/2017.-4., 08.2.2018. There is also practice of the Constitutional Court on violation of Article 35 and/or Article 36 of the Constitution due to such unreasoned warrants, see, e.g. U-III-1360/2014, 10.12.2019.

No further rules are prescribed in the CPA specifically as regards intepretation and presentation of electronic evidence.

The CPA sets out no special formal rule of evidence in assessment of facts:
"The right of the court and the state authorities participating in criminal proceedings to assess the existence or non-existence of facts shall not be bound or restricted by special formal rules of evidence" (Article 9, paragraph 1 of the CPA).

Evaluation of presented mobile forensic evidence by the court and assessment of its credibility / reliability is the same as with any other evidence.

Such evidence does not always need to be examined by expert witnesses (under Article 308 of the CPA, expertise shall be ordered when, in order to establish or assess some important fact it is necessary to obtain findings and an opinion of a person with the necessary expert knowledge or skills).

Expert witnesses under the CPA are not the same as other experts, such as: "expert assistants", which only provide assistance in the performance of certain evidentiary actions, such as, specifically, the "taking of measures to prevent the destruction or modification of data", upon order of the authority carrying out a search of a movable such as a mobile phone (Article 257, paragraph 2 of the CPA) or "experts", such as e.g. those requested by the State Attorny to clarify "certain technical or other expert issues that are raised concerning the evidence collected or during the taking of evidentiary actions" (Article 222, paragraph 3 of the CPA). Their statements, unlike those of expert witnesses, do not represent evidence in the proceedings. [114]

Related case law: The defendant claimed that the opinion and finding of expert witness was unlawful evidence, since that person was earlier in proceedings present at the evidentiary action of search of the movable (concretely: computer server). The court established that the search was not conducted by that expert witness, but by the police investigator who invited that person to be present in capacity of expert assistant. The court did not accept the request for disqualification as an expert witness.[115]

Apart from all earlier mentioned CPA rules, to the best of my knowledge there are no general rules and/or guidelines and/or common practices on the interpretation and presentation of

[114] Judicial Academy, Jozo Jurčević (Republic of Croatia State Attorney's Office); Marina Matušan (County State Attorney's Office in Split, Conduct of evidence by expertise in proceedings before the attorney attorney, court or administrative body (title in original language: Provođenje dokaza vještačenjem u postupku pred državnim odvjetnikom, sudom ili upravnim tijelom, September 2018, http://pak.hr/cke/obrazovni%20materijali/Provo%C4%91enje%20dokaza%20vje%C5%A1ta%C4%8Denjem%20u%20postupku%20pred%20dr%C5%BEavnim%20odvjetnikom.docx, p. 23.
[115] Supreme Court of Republic of Croatia, I Kž 366/2017-4, decision, 19.10.2017.

evidence from mobile forensics and/or centralised management of mobile forensic operations. In such circumstances, training is important, as well as availability of any relevant literature. For example, in the scope of the Judicial Academy in December 2016 the personnel at the County State's Attorney Office created training materials on IT expertise in criminal proceedings*:*

> "The main problems that arise when conducting these evidentiary actions are primarily the recognition of electronic evidence, given its nature, i.e. the fact that it is often invisible, and there is a danger that this evidence can be easily erased, altered, damaged or manipulated, and during further course of proceedings it is necessary to establish and confirm its authenticity. Also, given the variability of electronic evidence, it must be secured in such a way that it must be available for a longer period of time. Given all these circumstances, taking electronic evidence is particularly sensitive and that is why a guide called "Taking e-evidence"[116]) has been adopted. This guide sets out general principles for the handling of electronic evidence, with the key issues being how to ensure the legality of the proceedings and to ensure the integrity of the proceedings with the help of experts and trained officials, in order to ensure the legality. " [117]

However, there are no further details and/or reference on the mentioned guide itself in this training material. [118]

Mentioned training materials (December 2016) from the State Attorney's Office conclude that IT experts are rarely used, and if expertise is used, it is as a rule telecommunications expertise:

> "As a rule, when we have seized computers or mobile phones at our disposal, we decide on the evidentiary action of the search and our decision on the merits is based on the minutes of the search. The question here is whether it is enough to be satisfied with this evidentiary action, or whether it would be much more correct to order an IT expertise.
> There is also the question of contamination of evidence, and consequently the question of illegality of evidence that is the result of unprofessional handling during the seizure of material." [119]

Information on available training/education (up to 2017) in the wider scope of preventing and combatting cybercrime, including training on digital evidence forensics, is available at the

[116] Title in original language is: "Uzimanje e-dokaza".
[117] Judicial Academy, Križanić, Gordana (County State Attorney's Office in Karlovac), Expertise in criminal proceedings: IT expertise (title in original language: Vještačenje u kaznenom postupku - informatičko vještačenje), December 2016, http://pak.hr/cke/obrazovni%20materijali/Vje%C5%A1ta%C4%8Denje%20u%20kaznenom%20postupku.pdf, p. 30.
[118] Possibly it is the Council of Europe's Electronic Evidence Guide? For accuracy and further details I advise contacting the relevant author / State Attorney's Office.
[119] Judicial Academy, Križanić, Gordana (County State Attorney's Office in Karlovac), December 2016, http://pak.hr/cke/obrazovni%20materijali/Vje%C5%A1ta%C4%8Denje%20u%20kaznenom%20postupku.pdf, p. 33.

Evaluation report on Croatia in the scope of "The practical implementation and operation of European policies on prevention and combating cybercrime" (Council of the EU).[120]

In domestic literature (2016) there are examples of practices used in the seizing of computers / mobile phones / digital trace holders:

> "If computers or other electronic trace media to be seized are found during the search, the home screen on the device will be photographed (if the device is turned on), after which the device will be turned off and packaged in a way that the entire computer will be lined with paper, foil or in another way and sealed with an official seal in order to prevent the opening of the computer without removing the seal, and thus ensure the so-called unbroken chain of evidence, after which the computer is taken to the official premises of the police. The only difference is in the handling of mobile and similar devices, when the device will not be turned off (due to the possibility of password protection), but will be packed while turned on. Seizure of the computer or other electronic trace holder will be stated in the minutes of the search and a receipt on temporary seizure of items to the person undergoing the search, and if the computer or other holder of electronic traces is seized without a search, then in addition to the receipt on temporary seizure of items also minutes on temporary seizure of items will be made (no warrant). In this way, all formal conditions regarding the procedure of seizing the computer / digital trace holders have been met, and it will be possible to use them as evidence in possible court proceedings."

The author considered it extremely useful to have a standard operative procedure with steps to be taken when seizing the computer at the Ministry of the Interior.

In regard to the subsequent process of search (forensic investigation), the same author stated:

> "In the organizational unit of the police that initiated the entire procedure, the procedure is taken over by a police officer who has the highest level of knowledge of computer technology, although he/she does not necessarily have to be educated for that. Namely, in the system of the Ministry of the Interior there is no special program for training police officers in this area, but it all comes down to personal experience and knowledge of police officers, based on which the immediate superior should determine the competencies of the police officer.
> These indicators have resulted in each computer forensic investigator using different programs in their work and there is no prescribed standardization regarding software solutions in the processing of digital traces in the Republic of Croatia. This actually means that any computer forensic investigator can use any digital trace processing program, so although there are no written results of this mode of operation, it would be very interesting to see if the use of other, free forensic tools has effects on the efficiency and quality of the conduct of the evidentiary action of search of movable by police

[120] Council of the European Union, Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime"-Report on Croatia, 5250/1/17, REV 1 DCL 1, GENVAL3 CYBER9, 11.4. 2017, https://data.consilium.europa.eu/doc/document/ST-5250-2017-REV-1-DCL-1/en/pdf, pp. 92-97.

investigators, but also on the level of credibility of such traces in the later stages of criminal proceedings."[121]

According to the recently published news at the website of the Ministry of the Interior beginning of 2020, the project "Strengthening the capacity of the Ministry of the Interior in the fight against all forms of cybercrime" will enable procurement of necessary software and fardware as well as training on digital evidence and forensic methods and procedures for 31 police officers:

"As part of the project, the necessary equipment and computer programs will be procured that will enable the efficient execution of court orders for the search of electronic evidence holders. The Independent Sector for Schengen Coordination and European Union Funds of the Ministry of the Interior has decided to allocate financial resources for the implementation of the project: "Strengthening the capacity of the Ministry of the Interior in the fight against all forms of cybercrime." (….)
The project consists of two components:
1. Equipping the organizational units of the Ministry of the Interior with the necessary software and hardware components
2. Implementation of educational modules on digital evidence and forensic methods and procedures for 31 police officers
The project will procure the necessary equipment and computer programs that will enable the efficient execution of court orders to search electronic evidence carriers such as computers, tablets, hard disks and mobile phones. The aim of the training is to raise the competencies of police officers for the successful suppression of cybercrime. The training includes the following topics: Basics of attack and protection of information systems and information security; Information technology architecture, models, mechanisms and principles; Digital traces, evidence and forensics, and Prevention, surveillance and specialized areas of cyber attacks ..."[122]

Requirements for permanent court experts

Act on Courts (Official Gazette no. 28/13, 33/15, 82/15, 82/16, 67/18 and 126/19)

Article 125
Permanent court experts, based on their professional knowledge, provide the court with the service of providing an expert finding and opinion (expertise) when necessary in order to establish or clarify the facts established in the proceedings.

Article 126

[121] Nikola Protrka, Krešimir Filipić, Uloga forenzičkog softvera EnCase pri radu s elektroničkim tragovima (The role of forensic software EnCase with digital trace), Kriminalistička teorija i praksa, Vol. 3. No. 2/2016., 2016., pp. 121-134, at pp. 125-127. Text translated into English by researcher.
[122] Ministry of the Interior, https://mup.gov.hr/vijesti/aktivnosti-u-sklopu-projekta-jacanje-kapaciteta-mup-a-u-borbi-protiv-svih-oblika-kibernetickog-kriminaliteta/285974, 08.1.2020.

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

1) Judicial expertise shall be performed by legal or natural persons.
(2) A natural person with a completed professional study, undergraduate or graduate university study may be appointed as a permanent court expert. Exceptionally, a natural person who has completed secondary education in the relevant profession may also be appointed a permanent court expert.
(3) Legal persons may perform court expertise only within the scope of their registered activity, provided that this isperformed by their employees who meet the conditions referred to in paragraph 2 of this Article.
(4) Permanent court experts shall be appointed and dismissed by the president of the county or commercial court for his area. Permanent court experts are appointed for a term of four years and may be reappointed. Appointed permanent court experts may provide their services throughout the Republic of Croatia.
(6) The Minister of Justice shall prescribe by an ordinance the conditions and procedure for the appointment of permanent court experts, their rights and duties, as well as the amount of remuneration and reimbursement of expenses for their work.

According to Article 2 of the Ordinance on permanent court experts (Official Gazette no. 38/14, 123/15, 29/16 and 61/19), a person may be appointed as a permanent court expert, for whom it is determined that the following conditions in the appointment procedure have been met (emphasis added):

1. that he/she is a citizen of the Republic of Croatia, a citizen of a Member State of the European Union or a citizen of a state party to the Agreement on the European Economic Area,
2. that he/she is medically fit to perform the duties of a permanent court expert,
3. that after completing the appropriate study or appropriate school, he/she worked in the profession, as follows:
- at least 8 years - if he/she has completed graduate university studies or specialist graduate professional studies
- at least 10 years - if he/she has completed the appropriate undergraduate university study or undergraduate professional study
- at least 12 years - if he/she has completed the appropriate high school, and in case there is for a particular profession no appropriate undergraduate university study or undergraduate professional study or graduate university study or specialist graduate professional study
4. that he/she has successfully completed the exam on the structure of the judiciary, state administration and legal terminology
5. *that he/she has successfully completed professional training*
6. to have concluded a contract on insurance against liability for performing the duties of a permanent court expert,
7. to have a valid approval for independent performance of activities (license) or to have passed a professional or specialist exam for performing activities if this is a condition for performing these activities in accordance with special regulations.

A person for whom there are obstacles to admission to the civil service may not be appointed as a permanent court expert.

Professional training with a mentor

A candidate for a permanent court expert who passed the exam (on the structure of the judiciary, state administration and legal terminology) is referred by the president of the relevant court for professional training to the professional association of permanent court experts. Professional training, which last for up to a year, will be conducted according to a program determined for each activity or profession by the appropriate professional association, and approved by the Ministry of Justice. Professional associations are obliged to appoint mentors for professional training. A permanent court expert who has at least five years of experience in performing court expertise may be appointed as a mentor. The list of mentors is submitted to the county and commercial courts.

Continuous education/training

The permanent court expert is obliged to professionally improve and acquire professional knowledge in the field for which he / she has been appointed as a permanent court expert.[123]

Lists of permanent court experts

County and commercial courts keep a list of permanent court experts appointed for their area. A list of permanent court experts in Croatia, together with information on the competent court (county/commercial) and area of expertise (e.g. telecommunications - IT technology[124]) is available at the website of the Ministry of Justice.[125]

Selected provisions on expertise/expert witnesses in the CPA

Article 308
Expertise shall be ordered when, in order to establish or assess some important fact it is necessary to obtain findings and an opinion of a person with the necessary expert knowledge or skills.

Article 309
(1) Expertise shall be ordered in writing by the authority conducting the proceedings. The order shall specify the facts with respect to which expertise is to be performed and the name of the expert witness. The order shall also be served on the parties.
(2) If a specialised institution or a state authority exists for a certain type of expertise, such expertise, particularly a complex one, shall, as a rule, be entrusted to such an institution or authority. The institution or authority shall appoint one or more experts to conduct the expertise.

---

[123] Article 18 of the Ordinance on permanent court experts.
[124] A list of professional sections (Croatian Association of Court Expert Witnesses and Valuers) is available at:
[125]https://pravosudje.gov.hr/UserDocsImages/dokumenti/Pravo%20na%20pristup%20informacijama/Registri%20i%20baze%20podataka/Stalni%20sudski%20vje%C5%A1taci.pdf (last accessed 14.8.2020). Additionally, a list of legal entities performing court expertise and permanent court experts for all courts is published at the website of the Ministry of Justice: https://pravosudje.gov.hr/UserDocsImages/dokumenti/Pravo%20na%20pristup%20informacijama/Registri%20i%20baze%20podataka/Popis%20pravnih%20osoba%20koje%20imaju%20odobrenje%20za%20obavljanje%20sudskih%20vje%C5%A1ta%C4%8Denja.pdf (last accessed: 14.8. 2020).

(3) As a rule, one expert witness shall be appointed and if the expertise is a complex one, two or more expert witnesses shall be appointed.
(4) If for a certain type of expertise the court has permanently appointed expert witnesses, other expert witnesses may be appointed only where there is a risk of delay or where permanent expert witnesses are unable to perform the expertise when requested to do so or where other circumstances so require.

Article 310
(1) A person summoned as an expert witness is required to respond to the summons and present his or her finding and opinion.
(2) If a duly summoned expert witness fails to appear and does not justify his absence or if he refuses to perform the expertise, he may be fined in an amount not exceeding HRK 50,000.00 and in the case of an unjustified absence may be forcibly brought before the court. The decision on a fine and on forcible bringing before the court shall be rendered by the judge of investigation. An appeal against the order imposing a fine shall be decided by the panel.
(3) Notwithstanding the provisions of paragraph 2 of this Article, the authority conducting the proceedings may request from the expert witness to state the time limit by which he or she shall submit his or her findings and opinion.

Article 311
(1) A person who may not be interrogated as a witness or who is exempt from the duty to testify or against whom the criminal offence in question was committed may not be appointed as an expert witness and if such a person is appointed, his or her findings and opinion may not be used as evidence in the proceedings.
(2) Employment of a person with the same government authority or the same employer as the prosecutor, the defendant or the injured person is also the reason for his or her disqualification as an expert witness.
(3) As a rule, a person interrogated as a witness shall not be appointed an expert witness.

Article 312
(1) Before starting the expertise, the expert witness shall be asked to thoroughly examine the object of expertise, to accurately indicate everything he/she notices and discovers and to give an unbiased opinion which is in compliance with the rules of the science or skill in question. He/she shall in particular be warned that the giving of a false expert witness testimony is a criminal offence.
(2) An expert witness may be asked to swear to tell the truth. The oath reads: “I swear that I shall perform the expertise entrusted to me with due diligence and to the best of my knowledge and that I shall present my findings and state my opinion accurately, completely and objectively, in accordance with the rules of profession.” A permanently sworn expert witness shall only be reminded of this oath.
(3) An expert witness may be permitted to examine the file. He/she may suggest that objects and information that are of relevance to his/her findings and opinion be obtained. If he/she is present at the inspection or any other evidentiary action, the expert witness may suggest that certain circumstances be clarified or that the person interrogated be asked certain questions.
(4) The authority conducting the proceedings may be present when the expert witness takes actions.

Article 314
(1) The findings and the opinion of the expert witness shall be immediately entered into the protocol. The expert witness may be permitted to subsequently submit his/her findings and opinion in writing within the

time limit set by the authority conducting the proceedings, in a sufficient number of copies for the court and the parties.
(2) An expert witness may be interrogated via an audio-video device where this is provided for in a treaty or when both parties agree thereon.

Article 315
(1) If the task of performing an expertise is entrusted to an institution or government authority, the authority conducting the proceedings shall warn that the person referred to in Article 311 of this Act or a person with respect to whom there is a ground for disqualification from the conduct of an expertise as provided for in this Act may not participate in the reporting of any findings or the giving of an opinion and shall also warn of the consequences of reporting a false finding or giving a false opinion.
(2) The materials necessary for the conduct of an expertise shall be made available to the institution or government authority and, where necessary, it shall be proceeded according to the provisions of Article 313 of this Act.
(3) Written findings and opinion signed by persons who conducted the expertise shall be served by the relevant institution or government authority.
(4) At the request of a party, the head of the institution or government authority shall announce the names of experts who are to conduct the expertise in question.
(5) The provisions of Article 312, paragraphs 1through 3, of this Act shall not apply where the conduct of an expertise is entrusted to an institution or government authority. The authority conducting the proceedings may request that the institution or authority provide an explanation of the presented findings and opinion.

Article 316
(1) The protocol of the expertise or the written findings and opinion shall specify the name of the person who conducted the expertise in question as well as the occupation, educational background and field of specialisation of the expert witness.
(2) Where an expertise was conducted in the absence of the parties, the parties shall be notified that the expertise has been completed and that they may examine and collect the protocol of the expertise, and the written findings and opinion.

Article 317
Where the findings of an expert witness are unclear, incomplete or contradictory either among themselves or to the circumstances inquired and where these shortcomings cannot be remedied by reinterrogating the expert witness, expertise shall be reconducted by the same or another expert witness.

Article 318
Where the opinion of an expert witness is contradictory or has shortcomings or where there are grounds for doubting the accuracy of the opinion, and where these shortcomings or doubts cannot be remedied or removed by reinterrogating the expert witness, the opinion of another expert witness shall be requested.

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

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

Please see below answer to question 51.

***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.*

Established and recognised standardisation(s) of the processes: to the best of my knowledge, no. Not obligatory but possibly critical: please see explanations in answers 37 and 48 on the training materials and availability thereof. The possibility that "internal" documents/guidelines exist (e.g. at/for the State Attorney's Office, etc.) cannot be excluded.

***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.*

The Researcher's overview lays out a number of decisions in which the courts, when deciding on claims to exclude (separate) evidence from the file as unlawful, decided evidence to be lawful, but noted that all other related claims on such evidence (and on data derived from it) could be disputed further on in the proceedings on the basis of their reliability, which will be assessed by the court. Where needed, expertize can be ordered (under Article 308 of the CPA expertise shall be ordered when, in order to establish or assess some important fact it is necessary to obtain findings and an opinion of a person with the necessary expert knowledge or skills.). Mentioned cases are fairly recent and final judgments on the merits are awaited (to be issued and/or published).

Example:

Defendant's claims of questionable quality of photographed SMS messages and other mobile phone content by the police in a public space, which the wintess allowed voluntarily (and which action would not according to the Court fall under the CPA search provisions, and which mobile phone was not temporarily seized) are to be discussed as a matter of reliability before the court during proceedings, and they do not affect the legality of such data as evidence on which a court decision (charge: murder) cannot be based.[126]

The following case provides insight into practices that may give rise to claims of unreliable evidence (applied per analogiam to mobile phone devices), which have also been pointed to in the earlier mentioned training materials by the Judicial Academy. The Supreme Court in this case denied the request of the accused person for extraordinary review of final judgment, and according to this decision, claims on lack of reliability of evidence were discussed before the first and second instance court and expert examination was conducted, during which disputable issues were clarified:

"… the accused unsuccessfully complains about the legality of the search of the laptop […], stating that the laptop was not only the subject of the search but at the same time a means for the otherwise illegal search of the SD card, because the contents of that card were viewed on the laptop in question. This information, connected with an extremely unprofessional search of the laptop (which the applicant corroborates by claiming that no so-called backup was made on the computer before opening the files in the computer) resulted in the fact that during the expert examination it was no longer possible to determine whether files were opened [at a specific time period], including those that are the subject of the incrimination, which made it impossible to verify the authenticity of the testimony of witness.
The accused himself added that memory cards were inspected on his laptop which were found in the bag, instead of on another computer, which enabled the transfer of files from memory cards to the computer and vice versa, which means that after that neither the computer nor memory cards could be credible evidence due to suspicion of their contamination."

The Court confirmed the findings of both the first and second instance court, that the laptop was searched on the basis of a previously issued search warrant, so the defense's motion to separate the evidence as unlawful was properly rejected:

"The fact that on the same occasion, when the computer was searched, the SD memory card was searched on the same computer, for the search of which no warrant of the investigating judge was issued, so that part of the search record was separated as unlawful (by first and second instance court decisions), does not make the computer search illegal. These are two searches that each form a separate unit, and the fact that one protocol (minutes) was made of both did not result in a different qualification of these actions as separate evidence. Finally, illegality of the search of the SD memory card led to the exclusion of the part of search minutes related to search of that card. The question, however, whether and to what extent the

[126] Supreme Court of Republic of Croatia, I Kž 669/2018-4, 05.12.2018.

search of the SD memory card for which no warrant was issued by the investigating judge, could "contaminate" with its content the computer for which the warrant existed, is possibly an objection to the credibility of evidence, i.e., minutes of the computer search, which is essentially a question of fact, and on what grounds the filing of this extraordinary remedy is not permitted. Of the same meaning is the "unprofessional" way of conducting a computer search, which is explained in detail by the accused, i.e., the consequent inability to determine the earlier dates of access to individual files. The first-instance and second-instance courts commented on these allegations of the accused, which actually warn of certain shortcomings and shortcomings of the probative value of conducted search, after an expert examination was conducted, during which all disputable issues were clarified, since that is also a matter of objection on credibility of evidence, and not its lawfulness."

As regards the SD card, the Court noted that although it was searched unlawfully the first time, the card was searched subsequently upon the issued warrant and thus such latter search thereof was lawful: "the fact that content of the mentioned memory card was determined for the first time on the basis of an illegal search did not result in the illegality of the holder of that content - the SD memory card itself." [127]

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?*

During proceedings, a fairly common legal remedy used by the defendants is an appeal against a decision (order) of the court refusing to exclude from court files certain evidence which is allegedly unlawful (often - if obtained unlawfully). Commonly claims in appeals vis-à-vis evidence extracted via mobile forensics relate to substantive violations of the provisions of criminal procedure, in the sense that the decision which is being appealed is founded on unlawful evidence (Article 10), and that a grave violation of the right to a fair trial occurred, guaranteed by the Constitution and the European Convention on Human Rights (Article 468, paragraph 2 of the CPA). Furthermore, arguments observed in appeals relate also to substantive violations of the provisions of criminal procedure, in the sense that the court, in preparing or in the course of the trial or in rendering the decision, failed to apply or incorrectly applied any of the provisions of the Criminal Procedure Act or violated a right of the defence at the trial, provided that this influenced or could have influenced the decision (Article 468, paragraph 3 of the CPA).
Defendant's rights in criminal proceedings are, inter alia, to inspect the case file (right to go through, copy, photocopy and record the case file, examine items serving for the establishment of

[127] Supreme Court of the Republic of Croatia, judgment, III Kr 165/11-5, 19.9.2012.

the facts of the case)[128], to propose evidence and take part in evidentiary and other procedural acts as well as at the trial; to examine co-defendants, witnesses and expert witnesses, etc. (Article

[128] Article 183: (1) The right to inspect the case file shall include the right to go through, copy, photocopy and record the case file in accordance with the present Act and the State Attorney's file in accordance with a special act. The right to inspect the case file shall also include the examination of items serving for the establishment of the facts of the case. (2) Where proceedings are secret, in camera or with public excluded, only such persons as may participate in the said proceedings shall under the present Act have the right to inspect the case file. (3) Any data about a child participating in the proceedings as well as any data declared secret under a special act shall represent a secret. (4) Inspection of data that are secret shall be authorised in accordance with the provisions of this and a special act. (5) Where such concern as set forth in Article 294, paragraph 1, of the present Act exists, the judge of investigation shall, on the motion of the State Attorney or by virtue of his/her office, appropriately (by omitting from the copy of the minutes or the official notes any information on a person's identity, their singling out into a separate envelope or the like) protect the secrecy of information about the said persons which are in the case file. (6) Any person authorised to inspect the case file in the course of the inquiry, investigation or trial that has been declared secret shall be warned that he/she has a duty to keep secret any information that comes to his knowledge as well as the data referred to in paragraph 3 of this Article and that the disclosure of a secret is a criminal offence. This shall be noted in the case file being inspected, and shall be accompanied by the signature of the person warned. (7) Inspection of the case file shall be authorised and enabled by the body conducting the proceedings, unless otherwise provided by the present Act. After the conclusion of the proceedings, inspection of the case file shall be authorised by the president of the court or an official person designated by him. (8) Any person having a justified interest therein may be allowed inspection of the case file in accordance with law.
Article 184: (1) The parties shall have the right to inspect the case file. (2) The victim, injured party and their proxies shall have the right to inspect the case file. If prior inspection of the case file would influence the testimony of the victim or the injured party, they shall have the right to inspect the case file only after they have been examined. (3) The injured party as prosecutor shall have the right to inspect the case file after receipt of the notification referred to in Article 55, paragraph 1, of the present Act. (4) The defendant and defence counsel shall have the right to inspect the case file: 1) after the defendant is interrogated, if the interrogation is conducted before the issuance of the investigation order or before service of the notice referred to in Article 213, paragraph 2, of the present Act; 2) after service of the investigation order; 3) after service of the notice referred to in Article 213, paragraph 2, of the present Act; 4) after service of private action. (5) If an urgent evidentiary action has been taken with respect to a known defendant (Article 212 of the present Act) and the conditions set forth in paragraph 4 of this Article are not met, the defendant and defence counsel shall have the right to inspect the minutes of the taking of the said action no later than 30 days from the day the said action was taken.
Article 184a: (1) Where there is a risk that the inspection of the case file or a part thereof might jeopardise the purpose of the investigation by making it impossible or more difficult to gather important evidence, or where this would jeopardise life, limb or property of considerable value, the defendant may be denied the right to inspect the case file or a part thereof for a maximum of thirty days from service of the investigation order. Where no investigation is conducted, inspection of the case file or a part thereof may be denied for the reason that this would jeopardise life, limb or property of considerable value, for a maximum of thirty days from service of the notice referred to in Article 213, paragraph 2, of the present Act. (2) The decision on the denial of the right to inspection referred to in paragraph 1 of this Article until the indictment shall be taken by the State Attorney by an order that need not be reasoned. The defendant has the right to appeal the said order within three days. The appeal shall be filed with the State Attorney who shall deliver it without delay, together with the reasons for denying the inspection of the case file, to the judge of investigation. The defendant shall not be entitled to inspect the statement of reasons of the State Attorney. The appeal of the defendant shall be decided by the judge of investigation within 48 hours. The decision of the judge of investigation to refuse the defendant's appeal shall be served on the defendant without the statement of reasons and on the State Attorney with the statement of reasons. (3) If the revealing of evidence in

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

64). Defendant has the right to read the protocol / minutes (on the taking of evidentiary action such as search of a mobile phone)[129] and place objections.[130] He/she may appeal the order deciding on the motion of parties or on exclusion of evidence (Article 86)[131]. Defendant's right

---

proceedings for especially grave forms of criminal offences set forth in Article 334, items 1 and 2, of the present Act might jeopardise the investigation in these or other proceedings conducted against the same or other defendants or would put at risk the lives of other persons, the judge of investigation may, upon the motion of the State Attorney, issue an order denying the defendant until no later than the end of the investigation inspection of certain parts of the case file containing information on the said evidence. (4) If the defendant is in investigative prison, he/she may not be denied inspection of that part of the case file which is of relevance to the assessment of the existence of grounded suspicion that he/she committed a criminal offence and of the existence of circumstances giving grounds for the decision on the imposition or extension of investigative imprisonment.

[129] Article 82: (1) A protocol shall be drawn up about every action taken in the course of proceedings concurrently with the action's taking and where this is not possible, immediately afterwards. (2) The protocol shall be drawn up by the recorder. Only in cases of search of a home or of a person or where an action is taken outside the authority's official premises and the recorder is not available may the protocol be drawn up by the person taking the action in question. (3) Where the protocol is drawn up by recorder, it shall be drawn up in such a manner that the person taking the action dictates to recorder what he/she is to enter in the protocol. (4) The person being interrogated may be permitted to state answers directly on the protocol. In the case of abuse the said person may be denied this right.
Article 83: (1) The protocol shall contain the name of the government authority before which an action is taken, the location at which the said action is taken, the date and exact time when the action in question commences and ends, the names of the persons present, including in what capacity they are present, and the identification marking of the criminal case in which the action is taken. (2) The protocol must contain essential information on the course and contents of the action taken. Only the essential contents of statements and declarations made shall be entered in the protocol in the narrative form. Questions shall be recorded in the protocol only where this is necessary for understanding the answers. Where necessary, the question asked and the answer given to it shall be entered in the protocol verbatim. If objects and documents are seized in the course of taking an action, this shall be recorded in the protocol and the seized objects shall either be attached to the protocol or their location shall be stated. (3) When taking actions such as inspection, search, temporary seizure of objects or identification, information that is important in view of the significance of such an action or for determining the identity of certain objects (description, measures and size of objects or traces, marking of objects, etc.) shall also be entered in the protocol. Where sketches, drawings, blueprints, photographs, film or other technical recordings are made, this shall also be stated in the protocol and attached to it. (4) Special provisions on the protocol shall apply to the trial protocol (Articles 409 through 412), deliberation and voting protocols (Article 88) and other protocols as prescribed by this Act.
Article 84: (1) The protocol shall be taken in an orderly manner. There may be no additions or changes to it. The parts crossed out must remain legible. (2) All changes, corrections and additions shall be entered at the end of the protocol and shall be certified by the persons signing the protocol.

[130] Article 85: (1) The person interrogated, the persons whose presence during the taking of actions in the proceedings is mandatory and, if present, the parties, defence counsel and injured person shall be entitled to read the protocol or request that it be read to them. The person taking the action shall inform them of this right. A note shall be entered in the protocol as to whether this information was given to the persons in question as well as whether the protocol was read. The protocol shall always be read if no recorder is present and a note thereon shall be entered in the protocol. (…) (7) If objections are raised concerning the contents of the protocol, these objections shall be noted in the protocol as well.

[131] Article 86: (1) Upon the motion of the parties or by virtue of his office, the judge of investigation or the president of the indictment panel shall, respectively, by the end of the investigation or after receipt of the indictment for confirmation but before its examination (Article 344, paragraph 4) issue an order excluding any unlawful evidence

upon receipt of the investigation order is to file a motion with the State Attorney for the taking of evidentiary actions (Article 234).[132] He/she has the right to attend the evidentiary hearing and state remarks in the minutes, and to propose to the judge of investigation to ask for clarification purposes a witness or expert witness certain questions (Article 238).[133]At the trial, defendant is entitled to propose witnesses and expert witnesses and present evidence (Article 419, paragraph 1). After examining each of the witnesses or expert witnesses and after reading a document or presenting other evidence, the president of the panel shall ask the parties and the injured person

---

from the file. On the exclusion of any unlawful evidence the judge of investigation shall decide immediately and no later than three days from having learnt of the said evidence. The order deciding on the motion of the parties or on the exclusion of evidence shall be subject to special appeal. The appeal shall be decided by a higher court. (2) After the order becomes final the excluded evidence shall be enclosed in a special envelope and kept with the judge of investigation separate from the other files. They may not be inspected nor may they be used in the proceedings.

[132] Article 234 (1): Upon receipt of the investigation order, the defendant may file a motion with the State Attorney for the taking of evidentiary actions. If the State Attorney accepts the defendant's motion, he/she shall take the appropriate evidentiary action. The motion for the taking of an evidentiary action cannot be filed after the defendant is informed that the investigation has been completed (Article 228, paragraph 2). (2) If the State Attorney does not accept the defendant's motion, he/she shall deliver it within eight days to the judge of investigation and shall inform the defendant thereof in writing. If the judge of investigation accepts the motion for the taking of an evidentiary action, he/she shall order the State Attorney to take it, and if he/she does not, he/she shall inform the defendant thereof. (3) The defendant and defence counsel that filed the motion for the taking of the action referred to in paragraphs 1 and 2 of this Article shall be informed, prior to its taking, of the place and time of its taking. A defendant that has been deprived of liberty but wants to be present at the hearing shall be brought to the hearing, unless he/she is unfit to plead or due to severely undermined health is unable to take part in the hearing. If the defendant agrees to it and the technical conditions for it exist, the defendant shall be enabled to take part in the hearing via a closed remote communications device (audio-video device). (4) The defendant and defence counsel may be notified of the taking of the evidentiary action referred to in paragraphs 1 and 2 of this Article within a reasonable period of time via a telecommunications device, whereof an official note shall be made. (5) If the evidentiary action of witness or expert witness examination is being taken pursuant to paragraphs 1 and 2 of this Article, after the freely given testimony, questions shall first be put by the State Attorney and then by the defendant and defence counsel. The State Attorney shall prohibit the asking of the questions referred to in Article 420, paragraph 3, of the present Act and shall enter in the minutes the question and his decision.

[133] Article 238: (1) Where the State Attorney makes a motion for an evidentiary hearing, he must be present at the said hearing. (2) Unless otherwise prescribed for the action taken, the defendant, subsidiary prosecutor, defence counsel and injured person may attend an evidentiary hearing. The persons present at the evidentiary hearing may state their remarks to the minutes, which shall be noted at the end of the minutes (3) An evidentiary hearing cannot be held without the defence counsel if defence is mandatory. (4) The persons participating in the evidentiary hearing may propose to the judge of investigation to ask for clarification purposes a witness or expert witness certain questions. With the permission of the judge of investigation, they may also ask questions directly. (5) If the defendant is present at an evidentiary hearing, the judge of investigation must, upon opening the evidentiary hearing, check whether he received a written instruction on his rights (Article 239, paragraph 1). If the defendant did not receive the said instruction, the judge of investigation shall proceed as stated in Article 239, paragraph 3, of this Act, and if criminal prosecution was taken over by the subsidiary prosecutor, the judge of investigation shall serve the said instruction on the defendant. (6) During the course of an evidentiary hearing the judge of investigation may proceed as stipulated in Article 222, paragraph 3, of this Act (Note by researcher: may request from the relevant professional institution or an expert to be provided with the necessary explanations of certain technical or other expert issues raised concerning the evidence collected or during the taking of evidentiary actions).

whether they have any remarks concerning the evidence presented (Article 433), etc. Expert findings are subject to verification of credibility and legality, and any disputed credibility of expert findings is subject to the court's assessment as well as all other presented evidence. According to Article 317 (also CPA), where the findings of an expert witness are unclear, incomplete or contradictory either among themselves or to the circumstances inquired and where these shortcomings cannot be remedied by reinterrogating the expert witness, expertise shall be reconducted by the same or another expert witness. Also, under Article 318, where the opinion of an expert witness is contradictory or has shortcomings or where there are grounds for doubting the accuracy of the opinion, and where these shortcomings or doubts cannot be remedied or removed by reinterrogating the expert witness, the opinion of another expert witness shall be requested.

In cases of special evidentiary actions such a interception, collection, and recording of computer data (Article 332 of the CPA), the defendant has the right to have the recording reproduced or to have the transcript / documents inspected, and after the recording has been reproduced or the transcript or documents inspected, the defendant may propose at the trial that the recording, transcript or documents be reproduced or read out in full or in part (Article 338, paragraph 4).

In relation to formal requirements of the warrant for special evidentiary measures – secret telecommunication surveillance under the CPA, the European Court of Human Rights rendered several judgments against Croatia on violation of Article 8 of the European Convention on Human Rights. According to the Court such warrants did not provide adequate reasoning as to particular circumstances of the case and in particular reasons why the investigation (*inquiries into criminal offenses*) could not be conducted by other, less intrusive, means. Where the violation of a right to fair trial was also claimed (Article 6, para. 1. of the Convention), for example in the Dragojević case the European Court of Human Rights established there was no violation of that right as regards the use of impugned evidence obtained by secret surveillance:

„The applicant did not put forward arguments disputing reliability of information obtained by secret surveillance measures but limited his objection exclusively to the formal use of such information as evidence during the proceedings; the applicant had an effective opportunity to challenge the authenticity of the evidence and oppose its use and used that opportunity during the proceedings before the first-instance court, and in his appeal and constitutional complaint; domestic courts examined his arguments on the merits and provided reasons for their decisions; impugned evidence was not the only evidence on which the conviction was based. Thus the use of the impugned recordings in evidence did not as such deprive the applicant of a fair trial. [134]

There is also practice of the Constitutional Court on violation of Article 35 and/or Article 36 of the Constitution due to unreasoned warrants for special evidentiary measures, e.g. U-III-

[134] Points 131-135 of the judgment (Dragojević v. Croatia, no. 68955/11).

1360/2014, 10.12.2019. However, the right to a fair trial in Article 29 of the Constitution had not been violated. That right is according to the Court not absolute because in the assessment of each of the guarantees of a fair trial from Article 29 of the Constitution, the Court will consider the procedure as a single whole. In making such an assessment, the Court will consider the proceedings as a whole, including the manner in which the evidence was obtained, bearing in mind not only the rights of the defense but also the interest of the public and victims in the proper prosecution of criminal offenses. The Court found that during the entire criminal proceedings the applicant was represented by the chosen defense counsel and had the opportunity to propose evidence, comment on the evidentiary proceedings, give his view of the decisive facts, and point out all his objections. The courts of first and second instance duly reasoned their findings. The fact that the applicant was unsuccessful in no way alters the fact that he had an effective opportunity to challenge the evidence and to oppose its use. The fact that the warrants in question were not properly reasoned does not mean, in itself, that special evidentiary measures should not have been ordered in the circumstances of the particular case. In addition, the applicant did not dispute the veracity of the evidence gathered by special evidentiary measures. The Constitutional Court noted that the evidence obtained through the application of special evidentiary measures were not the only or decisive evidence against the applicant. The Constitutional Court considers that there is nothing to support the conclusion that the applicant's rights of defense were not adequately respected with regard to the evidence adduced or that the courts' assessment was arbitrary. In conclusion, the Constitutional Court found that, considering the criminal proceedings in question as a single unit, the applicant's right to a fair trial guaranteed by Article 29 para. 1 and 4 of the Constitution had not been violated.

In the following case the Supreme Court denied the request of the accused person for extraordinary review of final judgment. Claims on lack of reliability of evidence were discussed before the first and second instance court and expert examination was conducted, during which disputable issues were clarified:

"… the accused unsuccessfully complains about the legality of the search of the laptop […], stating that the laptop was not only the subject of the search but at the same time a means for the otherwise illegal search of the SD card, because the contents of that card were viewed on the laptop in question. This information, connected with an extremely unprofessional search of the laptop (which the applicant corroborates by claiming that no so-called backup was made on the computer before opening the files in the computer) resulted in the fact that during the expert examination it was no longer possible to determine whether files were opened [at a specific time period], including those that are the subject of the incrimination, which made it impossible to verify the authenticity of the testimony of witness.

The accused himself added that memory cards were inspected on his laptop which were found in the bag, instead of on another computer, which enabled the transfer of files from memory cards to the computer and vice versa, which means that after that neither the computer nor memory cards could be credible evidence due to suspicion of their contamination." (…)

"The fact that on the same occasion, when the computer was searched, the SD memory card was searched on the same computer, for the search of which no warrant of the investigating judge was issued, so that

part of the search record was separated as unlawful (by first and second instance court decisions), does not make the computer search illegal. These are two searches that each form a separate unit, and the fact that one protocol (minutes) was made of both did not result in a different qualification of these actions as separate evidence. Finally, illegality of the search of the SD memory card led to the exclusion of the part of search minutes related to search of that card. The question, however, whether and to what extent the search of the SD memory card for which no warrant was issued by the investigating judge, could "contaminate" with its content the computer for which the warrant existed, is possibly an objection to the credibility of evidence, i.e., minutes of the computer search, which is essentially a question of fact, and on what grounds the filing of this extraordinary remedy is not permitted. Of the same meaning is the "unprofessional" way of conducting a computer search, which is explained in detail by the accused, i.e., the consequent inability to determine the earlier dates of access to individual files. The first-instance and second-instance courts commented on these allegations of the accused, which actually warn of certain shortcomings and shortcomings of the probative value of conducted search, after an expert examination was conducted, during which all disputable issues were clarified, since that is also a matter of objection on credibility of evidence, and not its lawfulness."[135]

Where mobile phone/content was allegedly provided to the police voluntarily so that photographs would be made, courts must establish facts and issue a reasoned decision when denying defendant's claim to exclude such evidence as unlawful:

1) Where the police photographed mobile phones of witnesses, including a photography of a message on Facebook profile on the mobile phone of a witness, and the defendants claimed that such evidence (photo-documentation of the inspection: photography of the mobile phone of the witness and photography of a message on their Facebook profile) was unlawful, the courts, when denying such claims, must provide adequate argumentation for reaching their decision that the evidence is lawful and it is not enough to only state that the mobile phones in question were handed to the police voluntarily. The reasons for their decision and the way that the police obtained the mobile phones in question must be evident from court files and it must be established during trial (e.g. in questioning before the judge) if the mobile phones had been provided to the police voluntarily, if their owners unlocked them and thus enabled a search of their content (charge: murder). In the present case, therefore, the Supreme Court accepted the defendant's appeal to the lower court's decision refusing to exclude from court file as unlawful mentioned evidence thus obtained.[136]

2) Where it is not enough documented how the photographs of SMS messages were obtained by the police (in concrete case content of SMS both of the defendant and the injured party), i.e., it was only stated that the photo-documentation is classified as „inspection", the courts must, where they base their decisions also on such photographs justify their decision denying defendant's

[135] Supreme Court of Republic of Croatia, judgment, III Kr 165/11-5, 19.9.2012.
[136] Supreme Court of Republic of Croatia, decision, I Kž 111/16-4, 24.2.2016.

claim on unlawful evidence and exclusion from court file, whether during the trial upon defendant's claim on exclusion of such evidence or at the latest in the judgment. The right of a defendant to a reasoned court decision was breached. In the case at hand the Supreme Court as appelate court accepted the defendant's appeal, remanded the case to the court of first instance for retrial and instructed the court of first instance to provide adequate reasons. [137]

3) The defendant claimed illegality of evidence in form of a photographed mobile phone of the injured (aggrieved) party and SMS messages contained in it (allegedly provided voluntarily by the injured party to the police officers, not in context of a search). The first-instance court did not during the proceedings provide reasons for rejecting the defendant's motion on exclusion of such evidence as unlawful. It also did not state in the impugned verdict that the defendant proposed the exclusion of such evidence as illegal evidence, nor did it provide reasons for rejecting such a motion in the verdict itself. The first-instance court only stated arbitrarily in the minutes from the hearing that this would not be illegal evidence because it was not a search of a mobile phone owned by the injured party, which that injured party voluntarily handed to police officers so that they could take photographs of SMS messages. The appellate court, therefore, remanded the case to the court of first instance for retrial. In renewed procedure the court of first instance needs to also examine whether such evidence was obtained as fruit of a poisonous tree, i.e., as a consequence of illegal search of the defendant's mobile device, because of which that court excluded from court files the records from the defendant's mobile phone and details of calls.[138]

***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?*

There are generally prescribed duties of continuous training/education for judges, state attorneys etc., however, training required by law specifically as regards evidence coming from mobile forensics would in my opinion only apply to permanent court experts in the related specific field. To be more specific, permanent court experts are under Article 18 of the Ordinance on permanent court experts (Official Gazette no. 38/14, 123/15, 29/16 and 61/19) obliged to professionally improve and acquire professional knowledge in the field for which they have been appointed.[139]

The Judicial Academy conducts training of judicial officials, candidates for judicial officials, advisers and trainees in judicial bodies, other officials in the field and other participants in proceedings before judicial bodies such as permanent court experts. Invitations to participate in the workshops are addressed to the heads of judicial bodies, who submit applications for

[137] Supreme Court of Republic of Croatia, I Kž 329/2017-4, decision, 24.2.2016.
[138] County Court in Pula, decision, Kž-210/2017-7, 19.12.2017.
[139] Article 18 of the Ordinance on Permanent Court Experts (Official Gazette no. 38/14, 123/15, 29/16 and 61/19).

participation to the Academy (further information is available in the Act on Judicial Academy, Official Gazette 52/19, and related acts). As mentioned earlier, in the scope of the Academy in December 2016 the personnel the County State's Attorney Office created training materials on IT expertise in criminal proceedings[140] (please see related answers to questions 37 and 48.)

***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?*

The pre-determined time is as regards the search warrant issued by the judge of investigation, which must be executed within the time limit of three days from the date of its issue. After that, a search may no longer be conducted on the basis of the said warrant. The warrant must be immediately returned to the judge of investigation who shall make a note on it invalidating it (Article 242, paragraph 3 of the CPA).

In available expert literature it has been pointed out that, in practice, where ICT expertise is concerned (finding and opinion of expert witness), the time-limit for conducting expertise is 30 days or shorter. It was also pointed out that expert witnesses usually cannot immediately start the expertise upon receiving the court order, but only when they come into possession of objects required to carry out the expertise. Sometimes, if primary processing of the object was carried out by the geographically dislocated police adiministration (e.g. search) in relation to the one which is competent by seat of the court or expert witness, it takes a couple of days to locate objects and have their delivery worked out to the police administration closer to the court or expert, etc. In certain types of cases the problem of insufficient deadline for the expertise are particularly evident, e.g. when during investigation expertise is ordered by the State Attorney, due to procedural circumstances expert witnesses sometimes have a time-limit of only 3 days to carry out the expertise.[141]

In cases of *special evidentiary actions* (Article 332 of the CPA), the warrant states the time limit that must be appropriate for achieving the goal (as well as the manner, scope and place of taking

[140] Judicial Academy, Križanić, Gordana (County State Attorney's Office in Karlovac), Expertise in criminal proceedings: IT expertise (title in original language: Vještačenje u kaznenom postupku - informatičko vještačenje), December 2016, http://pak.hr/cke/obrazovni%20materijali/Vje%C5%A1ta%C4%8Denje%20u%20kaznenom%20postupku.pdf, p. 30.
[141] Stokić Matija, Vještačenje u predmetima protupravnih radnji izvršenih uz uporabu informatičko-komunikacijske tehnologije (translation into English by researcher: Expertise in cases of illegal actions committed with the use of information and communication technology), IUS-INFO, 26.9.2017, p. 6.

the action). Special evidentiary actions shall be ordered for a period of up to three months, and they may be extended under prescribed circumstances (Article 335). These actions are executed by the police. The police prepares daily reports and technical transcripts on the course of their execution which it shall deliver to the State Attorney on his request. At any moment during the taking of the special evidentiary actions the judge of investigation may request from the State Attorney to deliver to him a report on the course of the said actions and the need for their further taking. During the taking of special evidentiary actions the judge of investigation may, where necessary, request from the police to have daily reports and technical transcripts delivered to him for the purpose of assessing the well-foundedness of their further taking, within the scope and to the extent which he himself determines. If the actions were extended by six months (pursuant to Article 335, paragraph 3), after three months the judge of investigation must request from the State Attorney to deliver to him the report on the need for their further taking. Upon expiry of the period for which the said actions were approved, the police shall draw up a special report for the State Attorney's Office and the judge of investigation in which it shall specify: 1. the dates and times the action in question started and ended; 2. the number and identity of persons with respect to whom the action in question was taken. (Article 337, paragraphs 1-2 of the CPA).

***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.)?*

Defendant's rights in criminal proceedings are, inter alia, to inspect the case file; to propose evidence and take part in evidentiary and other procedural acts as well as at the trial; to examine co-defendants, witnesses and expert witnesses, etc. (Article 64 of the CPA).

Victim of a criminal offence under the CPA is the physical person who has suffered physical and mental health consequences, pecuniary damage or a substantial violation of his/her fundamental rights and freedoms as a direct consequence of the criminal offence. The victim of a criminal offence is also the spouse, common-law spouse, life partner or informal life partner, descendant, and if there are no descendants, ancestor and sibling of the person whose death is the direct consequence of the criminal offence and the person whom the latter was required by law to maintain (Article 202, paragraph 2, item 11 of the CPA).

Injured party under the CPA is the victim of a criminal offence and the legal person to whose detriment the criminal offence was committed, which participate as the injured parties in the proceeding (Article 202, paragraph 2, item 12 of the CPA).

The injured party's rights in criminal proceedings are, inter alia, to: draw attention to facts and propose evidence; be present at the evidentiary hearing; be present at the trial, take part in evidentiary proceedings and deliver the closing argument; inspect the case file (pursuant to Article 184, paragraph 2); request to be informed by the State Attorney of the acts taken

following his report (Article 206a) and file a complaint to the senior State Attorney (Article 206b); take over criminal prosecution in lieu of the State Attorney (Article 55), etc. (Article 51 of the CPA).

Rights of the defendant and injured person regarding the protocol[142] (e.g. protocol on the taking of evidentiary action such as search of a mobile phone): reading the protocol, placing objections.[143]

Appealing the order deciding on the motion of parties or on exclusion of evidence (Article 86)[144]

---

[142] Article 82: (1) A protocol shall be drawn up about every action taken in the course of proceedings concurrently with the action's taking and where this is not possible, immediately afterwards. (2) The protocol shall be drawn up by the recorder. Only in cases of search of a home or of a person or where an action is taken outside the authority's official premises and the recorder is not available may the protocol be drawn up by the person taking the action in question. (3) Where the protocol is drawn up by recorder, it shall be drawn up in such a manner that the person taking the action dictates to recorder what he/she is to enter in the protocol. (4) The person being interrogated may be permitted to state answers directly on the protocol. In the case of abuse the said person may be denied this right.
Article 83: (1) The protocol shall contain the name of the government authority before which an action is taken, the location at which the said action is taken, the date and exact time when the action in question commences and ends, the names of the persons present, including in what capacity they are present, and the identification marking of the criminal case in which the action is taken. (2) The protocol must contain essential information on the course and contents of the action taken. Only the essential contents of statements and declarations made shall be entered in the protocol in the narrative form. Questions shall be recorded in the protocol only where this is necessary for understanding the answers. Where necessary, the question asked and the answer given to it shall be entered in the protocol verbatim. If objects and documents are seized in the course of taking an action, this shall be recorded in the protocol and the seized objects shall either be attached to the protocol or their location shall be stated. (3) When taking actions such as inspection, search, temporary seizure of objects or identification, information that is important in view of the significance of such an action or for determining the identity of certain objects (description, measures and size of objects or traces, marking of objects, etc.) shall also be entered in the protocol. Where sketches, drawings, blueprints, photographs, film or other technical recordings are made, this shall also be stated in the protocol and attached to it. (4) Special provisions on the protocol shall apply to the trial protocol (Articles 409 through 412), deliberation and voting protocols (Article 88) and other protocols as prescribed by this Act.
Article 84: (1) The protocol shall be taken in an orderly manner. There may be no additions or changes to it. The parts crossed out must remain legible. (2) All changes, corrections and additions shall be entered at the end of the protocol and shall be certified by the persons signing the protocol.

[143] Article 85: (1) The person interrogated, the persons whose presence during the taking of actions in the proceedings is mandatory and, if present, the parties, defence counsel and injured person shall be entitled to read the protocol or request that it be read to them. The person taking the action shall inform them of this right. A note shall be entered in the protocol as to whether this information was given to the persons in question as well as whether the protocol was read. The protocol shall always be read if no recorder is present and a note thereon shall be entered in the protocol. (…) (7) If objections are raised concerning the contents of the protocol, these objections shall be noted in the protocol as well.

[144] Article 86: (1) Upon the motion of the parties or by virtue of his office, the judge of investigation or the president of the indictment panel shall, respectively, by the end of the investigation or after receipt of the indictment for confirmation but before its examination (Article 344, paragraph 4) issue an order excluding any unlawful evidence from the file. On the exclusion of any unlawful evidence the judge of investigation shall decide immediately and no

Child as injured party (Article 53): special guardian /statutory representative.[145]

Rights of victim who took over criminal prosecution: same rights as the State Attorney, except such rights as the State Attorney has as a government body (Article 58, paragraph 1).

The right to inspect the case file (Articles 183-184a) - right to go through, copy, photocopy and record the case file, includes the examination of items serving for the establishment of the facts of the case.[146] Any data about a child participating in the proceedings as well as any data declared secret under a special act shall represent a secret (Article 183, paragraph 3).

---

later than three days from having learnt of the said evidence. The order deciding on the motion of the parties or on the exclusion of evidence shall be subject to special appeal. The appeal shall be decided by a higher court. (2) After the order becomes final the excluded evidence shall be enclosed in a special envelope and kept with the judge of investigation separate from the other files. They may not be inspected nor may they be used in the proceedings.

[145] Article 53: (1) Where the injured party is a child and the interests of the child are contrary to the interests of the parents, the body conducting the proceeding shall instruct the competent welfare body to appoint a special guardian for the child. (2) If the injured party is a child or a person deprived of contractual capacity, his statutory representative or special guardian shall be authorised to give all statements and take all actions to which the injured party is authorised under the present Act. (3) By way of derogation from the provision of paragraph 2 of this Article, an injured party that has attained the age of sixteen years may himself/herself give statements and take actions in the proceedings.

[146] Article 183: (1) The right to inspect the case file shall include the right to go through, copy, photocopy and record the case file in accordance with the present Act and the State Attorney's file in accordance with a special act. The right to inspect the case file shall also include the examination of items serving for the establishment of the facts of the case. (2) Where proceedings are secret, in camera or with public excluded, only such persons as may participate in the said proceedings shall under the present Act have the right to inspect the case file. (3) Any data about a child participating in the proceedings as well as any data declared secret under a special act shall represent a secret. (4) Inspection of data that are secret shall be authorised in accordance with the provisions of this and a special act. (5) Where such concern as set forth in Article 294, paragraph 1, of the present Act exists, the judge of investigation shall, on the motion of the State Attorney or by virtue of his/her office, appropriately (by omitting from the copy of the minutes or the official notes any information on a person's identity, their singling out into a separate envelope or the like) protect the secrecy of information about the said persons which are in the case file. (6) Any person authorised to inspect the case file in the course of the inquiry, investigation or trial that has been declared secret shall be warned that he/she has a duty to keep secret any information that comes to his knowledge as well as the data referred to in paragraph 3 of this Article and that the disclosure of a secret is a criminal offence. This shall be noted in the case file being inspected, and shall be accompanied by the signature of the person warned. (7) Inspection of the case file shall be authorised and enabled by the body conducting the proceedings, unless otherwise provided by the present Act. After the conclusion of the proceedings, inspection of the case file shall be authorised by the president of the court or an official person designated by him. (8) Any person having a justified interest therein may be allowed inspection of the case file in accordance with law.
Article 184: (1) The parties shall have the right to inspect the case file. (2) The victim, injured party and their proxies shall have the right to inspect the case file. If prior inspection of the case file would influence the testimony of the victim or the injured party, they shall have the right to inspect the case file only after they have been examined. (3)

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

Victim and injured party: right to request from the State Attorney to be informed of the actions taken pursuant to the crime report or the report on a committed offence (Article 206a).[147]

The injured party as prosecutor shall have the right to inspect the case file after receipt of the notification referred to in Article 55, paragraph 1, of the present Act. (4) The defendant and defence counsel shall have the right to inspect the case file: 1) after the defendant is interrogated, if the interrogation is conducted before the issuance of the investigation order or before service of the notice referred to in Article 213, paragraph 2, of the present Act; 2) after service of the investigation order; 3) after service of the notice referred to in Article 213, paragraph 2, of the present Act; 4) after service of private action. (5) If an urgent evidentiary action has been taken with respect to a known defendant (Article 212 of the present Act) and the conditions set forth in paragraph 4 of this Article are not met, the defendant and defence counsel shall have the right to inspect the minutes of the taking of the said action no later than 30 days from the day the said action was taken.

Article 184a: (1) Where there is a risk that the inspection of the case file or a part thereof might jeopardise the purpose of the investigation by making it impossible or more difficult to gather important evidence, or where this would jeopardise life, limb or property of considerable value, the defendant may be denied the right to inspect the case file or a part thereof for a maximum of thirty days from service of the investigation order. Where no investigation is conducted, inspection of the case file or a part thereof may be denied for the reason that this would jeopardise life, limb or property of considerable value, for a maximum of thirty days from service of the notice referred to in Article 213, paragraph 2, of the present Act. (2) The decision on the denial of the right to inspection referred to in paragraph 1 of this Article until the indictment shall be taken by the State Attorney by an order that need not be reasoned. The defendant has the right to appeal the said order within three days. The appeal shall be filed with the State Attorney who shall deliver it without delay, together with the reasons for denying the inspection of the case file, to the judge of investigation. The defendant shall not be entitled to inspect the statement of reasons of the State Attorney. The appeal of the defendant shall be decided by the judge of investigation within 48 hours. The decision of the judge of investigation to refuse the defendant's appeal shall be served on the defendant without the statement of reasons and on the State Attorney with the statement of reasons. (3) If the revealing of evidence in proceedings for especially grave forms of criminal offences set forth in Article 334, items 1 and 2, of the present Act might jeopardise the investigation in these or other proceedings conducted against the same or other defendants or would put at risk the lives of other persons, the judge of investigation may, upon the motion of the State Attorney, issue an order denying the defendant until no later than the end of the investigation inspection of certain parts of the case file containing information on the said evidence. (4) If the defendant is in investigative prison, he/she may not be denied inspection of that part of the case file which is of relevance to the assessment of the existence of grounded suspicion that he/she committed a criminal offence and of the existence of circumstances giving grounds for the decision on the imposition or extension of investigative imprisonment.

[147] Article 206a: (1) Upon expiry of two months from the submission of the crime report or the report on a committed offence the victim and the injured party have the right to request from the State Attorney to be informed of the actions taken pursuant to the crime report or the report on a committed offence. Unless the efficiency of proceedings would thereby be jeopardised, the State Attorney shall inform them within reasonable time and no later than thirty days from receipt of request of the actions taken. Of the denial to provide information the State Attorney shall inform the victim and the injured party that requested the said information. (2) If the State Attorney fails to inform the victim or the injured party or if the victim or the injured party are not satisfied with the information provided or the actions taken, they shall have the right to file a complaint to the senior State Attorney. (3) The senior State Attorney shall verify the allegations made in the complaint and if he establishes that the complaint is well-founded, he shall order the lower-ranking State Attorney to deliver to the person that lodged the complaint the requested information on the actions taken or to take within reasonable time any action which should have been taken. If the senior State Attorney establishes that as a result of the acts of the lower-ranking State Attorney the rights of the person that lodged the complaint have been violated, he/she shall inform the latter thereof and in doing so specify which rights have been violated. (4) Unless they have lodged a complaint with the senior State Attorney referred to in Article

Victim that took over criminal prosecution: right to file the motion for the taking of evidentiary actions (Article 213 c).[148]

During investigation phase, the injured person may submit to the State Attorney proposals that the investigation be supplemented, including other proposals for the purpose of exercising the rights prescribed by law, and may participate in investigatory actions and exercise the rights referred to in Article 51, paragraph 1 of the CPA, such as, proposing evidence (Article 221).

The victim as subsidiary prosecutor in prescribed circumstances has the right to file a motion with the judge of investigation to conduct an investigation into the criminal offence for which the investigation is conducted, which motion includes his/her proposal of evidentiary actions. The subsidiary prosecutor may be present during the taking of investigatory actions in the investigation and may file a motion with the judge of investigation asking him to order the investigator to take certain actions. The judge of investigation shall inform the subsidiary prosecutor in case he/she denies his/her motion for the taking of actions.[149]

206b, paragraph 2, of the present Act, the victim and the injured party may upon expiry of six months from the previously submitted request for information on the actions taken, make a new request for information on conducted actions set forth in paragraph 1 of this Article.

[148] Article 213c: (1) If the State Attorney dismisses the crime report for a criminal offence punishable by a fine or by imprisonment for up to five years, the victim that took over criminal prosecution may file with the judge of investigation a motion for the taking of evidentiary actions. The motion for the taking of evidentiary actions shall contain the data referred to in Article 225, paragraph 1, of the present Act. The decision of the judge of investigation on the subsidiary prosecutor's motion shall be taken in the form of an order. (2) If the the judge of investigation accepts the motion of the subsidiary prosecutor referred to in paragraph 1 of this Article, he/she shall order the investigator to take those evidentiary actions that are expedient for deciding on the preferment of the indictment. In taking the evidentiary actions it shall be proceeded as provided for in Article 225, paragraph 4, of the present Act. (3) If he/she does not accept the motion referred to in paragraph 1 of this Article, the judge of investigation shall issue an order rejecting it. (4) Upon the conclusion of the evidentiary actions, the judge of investigation shall proceed as provided for in Article 225, paragraph 5, of the present Act.

[149] Article 225: (1) If the State Attorney dismissed the crime report or discontinued the investigation, the victim that took over criminal prosecution may file a motion with the judge of investigation to conduct an investigation into the criminal offence for which the investigation is conducted. The motion to conduct the investigation must include the name of the State Attorney's Office that issued the order dismissing the crime report and the designation of the said order or the designation of the order discontinuing the investigation, a description of the act from which the statutory elements of a criminal offence are deducible, the statutory name of the criminal offence, a brief exposition of the circumstances giving rise to reasonable grounds for suspicion that the defendant committed the criminal offence and the proposed evidentiary actions. (2) The judge of investigation shall decide on the motion of the subsidiary prosecutor by an order. The order for the conduct of an investigation shall include the information referred to in Article 217, paragraph 2, of the present Act and specify the evidentiary actions whose taking the judge of investigation deems expedient. (3) If he/she does not accept the motion referred to in paragraph 1 of this Article, the judge of investigation shall issue an order rejecting the subsidiary prosecutor's motion for the conduct of an investigation. (4) If the subsidiary prosecutor’s motion for the conduct of the investigation is accepted, the investigation shall be conducted by the investigator upon the order of the judge of investigation. The subsidiary prosecutor may be present during the taking of investigatory actions in the investigation and may file a motion with

Defendant's right upon receipt of the investigation order is to file a motion with the State Attorney for the taking of evidentiary actions (Article 234).[150]

Defendant, victim as subsidiary prosecutor and injured person have the right to attend the evidentiary hearing and state remarks in the minutes, and to propose to the judge of investigation to ask for clarification purposes a witness or expert witness certain questions (Article 238).[151]

---

the judge of investigation asking him to order the investigator to take certain actions. The judge of investigation shall inform the subsidiary prosecutor in case he/she denies his/her motion for the taking of actions. (5) When the judge of investigation establishes that the investigation has been completed, he shall inform the subsidiary prosecutor thereof. The judge of investigation shall notify the subsidiary prosecutor of the location of the file and other objects and of the time when he/she may examine them as well as of his right to prefer an indictment within the time limit of eight days and his/her duty to inform the judge of investigation thereof. If the subsidiary prosecutor fails to prefer the indictment within the said period, it shall be deemed that he/she has desisted from prosecution and the judge of investigation shall issue an order discontinuing proceedings.

[150] Article 234: (1) Upon receipt of the investigation order, the defendant may file a motion with the State Attorney for the taking of evidentiary actions. If the State Attorney accepts the defendant's motion, he/she shall take the appropriate evidentiary action. The motion for the taking of an evidentiary action cannot be filed after the defendant is informed that the investigation has been completed (Article 228, paragraph 2). (2) If the State Attorney does not accept the defendant's motion, he/she shall deliver it within eight days to the judge of investigation and shall inform the defendant thereof in writing. If the judge of investigation accepts the motion for the taking of an evidentiary action, he/she shall order the State Attorney to take it, and if he/she does not, he/she shall inform the defendant thereof. (3) The defendant and defence counsel that filed the motion for the taking of the action referred to in paragraphs 1 and 2 of this Article shall be informed, prior to its taking, of the place and time of its taking. A defendant that has been deprived of liberty but wants to be present at the hearing shall be brought to the hearing, unless he/she is unfit to plead or due to severely undermined health is unable to take part in the hearing. If the defendant agrees to it and the technical conditions for it exist, the defendant shall be enabled to take part in the hearing via a closed remote communications device (audio-video device). (4) The defendant and defence counsel may be notified of the taking of the evidentiary action referred to in paragraphs 1 and 2 of this Article within a reasonable period of time via a telecommunications device, whereof an official note shall be made. (5) If the evidentiary action of witness or expert witness examination is being taken pursuant to paragraphs 1 and 2 of this Article, after the freely given testimony, questions shall first be put by the State Attorney and then by the defendant and defence counsel. The State Attorney shall prohibit the asking of the questions referred to in Article 420, paragraph 3, of the present Act and shall enter in the minutes the question and his decision.

[151] Article 238: (1) Where the State Attorney makes a motion for an evidentiary hearing, he must be present at the said hearing. (2) Unless otherwise prescribed for the action taken, the defendant, subsidiary prosecutor, defence counsel and injured person may attend an evidentiary hearing. The persons present at the evidentiary hearing may state their remarks to the minutes, which shall be noted at the end of the minutes (3) An evidentiary hearing cannot be held without the defence counsel if defence is mandatory. (4) The persons participating in the evidentiary hearing may propose to the judge of investigation to ask for clarification purposes a witness or expert witness certain questions. With the permission of the judge of investigation, they may also ask questions directly. (5) If the defendant is present at an evidentiary hearing, the judge of investigation must, upon opening the evidentiary hearing, check whether he received a written instruction on his rights (Article 239, paragraph 1). If the defendant did not receive the said instruction, the judge of investigation shall proceed as stated in Article 239, paragraph 3, of this Act, and if criminal prosecution was taken over by the subsidiary prosecutor, the judge of investigation shall serve the said instruction on the defendant. (6) During the course of an evidentiary hearing the judge of investigation may

At the trial, parties are entitled to propose witnesses and expert witnesses and present evidence (Article 419, paragraph 1).

No facts related to the victim's former sexual conduct or his/her sexual inclinations may be used as evidence in proceedings (Article 422, paragraph 1 - with exceptions in paragraph 2).

After examining each of the witnesses or expert witnesses and after reading a document or presenting other evidence, the president of the panel shall ask the parties and the injured person whether they have any remarks concerning the evidence presented (Article 433)

Before proceeding with the questioning of an accused who under Article 416, paragraph 5, of this Act is to be questioned at the close of evidentiary proceedings, the president of the panel shall ask the parties and the injured person whether they have any motions for the supplementing of evidentiary proceedings with evidence (Article 434, paragraph 1).

In cases of special evidentiary actions such a interception, collection, and recording of computer data (Article 332), the defendant has the right to have the recording reproduced or to have the transcript / documents inspected, and after the recording has been reproduced or the transcript or documents inspected, the defendant may propose at the trial that the recording, transcript or documents be reproduced or read out in full or in part (Article 338, paragraph 4 of the CPA).

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?*

In addition to specified rules in the CPA, no - to the best of my knowledge. Please see detailed explanations in answers 37 and 48. The possibility that "internal" documents/guidelines exist cannot be excluded.

---

proceed as stipulated in Article 222, paragraph 3, of this Act (Researcher's note: may request from the relevant professional institution or an expert to be provided with the necessary explanations of certain technical or other expert issues raised concerning the evidence collected or during the taking of evidentiary actions).

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.*

In essence the courts review defendants' claims on exclusion of evidence from the point of view of legality by taking into account explicit provisions of the CPA on unlawfully obtained evidence (for example, in cases of evidence obtained by search: whether alleged circumstance pointing to violation is stipulated in Article 250 of the CPA). Objections, such as on aproaches and methods used (where lawful, of course), and claims such as "extremely unprofessional search of the laptop" and contamination of searched computer"[152], "poorly done expertise not respecting professional rules"[153] or "questionable quality of photographed SMS messages and other mobile phone content" [154] have in practice mainly been examined from the point of view of reliability of evidence.

Expert findings are subject to verification of credibility and legality, and any disputed credibility of expert findings is subject to the court's assessment as well as all other presented evidence. Courts may order expertise in order to establish or assess some important fact it is necessary to obtain findings and an opinion of a person with the necessary expert knowledge or skills. According to Article 317 of the CPA, where the findings of an expert witness are unclear, incomplete or contradictory either among themselves or to the circumstances inquired and where these shortcomings cannot be remedied by reinterrogating the expert witness, expertise shall be reconducted by the same or another expert witness. Also, under Article 318 of the CPA, where the opinion of an expert witness is contradictory or has shortcomings or where there are grounds for doubting the accuracy of the opinion, and where these shortcomings or doubts cannot be remedied or removed by reinterrogating the expert witness, the opinion of another expert witness shall be requested.

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

For example, the Court examines the protocol / minutes of the search, and where necessary (e.g. upon party's motions) seeks clarifications (questioning of witnesses, for example), and where necessary it may order an expertise to establish or assess an important fact.

---

[152] Supreme Court of Republic of Croatia, judgment, III Kr 165/11-5, 19.9.2012.
[153] Supreme Court of Republic of Croatia, I Kž 536/2017-4, 8.11.2017.
[154] Supreme Court of Republic of Croatia, I Kž 669/2018-4, 05.12.2018.

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

"… the accused unsuccessfully complains about the legality of the search of the laptop […], stating that the laptop was not only the subject of the search but at the same time a means for the otherwise illegal search of the SD card, because the contents of that card were viewed on the laptop in question. This information, connected with an extremely unprofessional search of the laptop (which the applicant corroborates by claiming that no so-called backup was made on the computer before opening the files in the computer) resulted in the fact that during the expert examination it was no longer possible to determine whether files were opened [at a specific time period], including those that are the subject of the incrimination, which made it impossible to verify the authenticity of the testimony of witness.
The accused himself added that memory cards were inspected on his laptop which were found in the bag, instead of on another computer, which enabled the transfer of files from memory cards to the computer and vice versa, which means that after that neither the computer nor memory cards could be credible evidence due to suspicion of their contamination."

The Court confirmed the findings of both the first and second instance court, that the laptop was searched on the basis of a previously issued search warrant, so the defense's motion to separate the evidence as unlawful was properly rejected.

"The fact that on the same occasion, when the computer was searched, the SD memory card was searched on the same computer, for the search of which no warrant of the investigating judge was issued, so that part of the search record was separated as unlawful (by first and second instance court decisions), does not make the computer search illegal. These are two searches that each form a separate unit, and the fact that one protocol (minutes) was made of both did not result in a different qualification of these actions as separate evidence. Finally, illegality of the search of the SD memory card led to the exclusion of the part of search minutes related to search of that card. The question, however, whether and to what extent the search of the SD memory card for which no warrant was issued by the investigating judge, could "contaminate" with its content the computer for which the warrant existed, is possibly an objection to the credibility of evidence, i.e., minutes of the computer search, which is essentially a question of fact, and on what grounds the filing of this extraordinary remedy is not permitted. Of the same meaning is the "unprofessional" way of conducting a computer search, which is explained in detail by the accused, i.e., the consequent inability to determine the earlier dates of access to individual files. The first-instance and second-instance courts commented on these allegations of the accused, which actually warn of certain shortcomings and shortcomings of the probative value of conducted search, after an expert examination was conducted, during which all disputable issues were clarified, since that is also a matter of objection on credibility of evidence, and not its lawfulness."
As regards the SD card, the Court noted that although it was searched unlawfully the first time, the card was searched subsequently upon the issued warrant and thus such latter search thereof was lawful: "the fact that content of the mentioned memory card was determined for the first time

on the basis of an illegal search did not result in the illegality of the holder of that content - the SD memory card itself."[155]

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.*

The protocol (minutes) of the search normally specify the process used to acquire evidence and tools used, and the defense may ask questions thereon. Defendant's rights in criminal proceedings are, inter alia, to inspect the case file; to propose evidence and take part in evidentiary and other procedural acts as well as at the trial; to examine co-defendants, witnesses and expert witnesses, etc. (Article 64 of the CPA). For example, the right to inspect the case file *(*Articles 183-184a) includes the right to go through, copy, photocopy and record the case file, and it includes the examination of items serving for the establishment of the facts of the case.[156]

[155] Supreme Court of Republic of Croatia, judgment, III Kr 165/11-5, 19.9.2012.

[156] Article 183: (1) The right to inspect the case file shall include the right to go through, copy, photocopy and record the case file in accordance with the present Act and the State Attorney's file in accordance with a special act. The right to inspect the case file shall also include the examination of items serving for the establishment of the facts of the case. (2) Where proceedings are secret, in camera or with public excluded, only such persons as may participate in the said proceedings shall under the present Act have the right to inspect the case file. (3) Any data about a child participating in the proceedings as well as any data declared secret under a special act shall represent a secret. (4) Inspection of data that are secret shall be authorised in accordance with the provisions of this and a special act. (5) Where such concern as set forth in Article 294, paragraph 1, of the present Act exists, the judge of investigation shall, on the motion of the State Attorney or by virtue of his/her office, appropriately (by omitting from the copy of the minutes or the official notes any information on a person's identity, their singling out into a separate envelope or the like) protect the secrecy of information about the said persons which are in the case file. (6) Any person authorised to inspect the case file in the course of the inquiry, investigation or trial that has been declared secret shall be warned that he/she has a duty to keep secret any information that comes to his knowledge as well as the data referred to in paragraph 3 of this Article and that the disclosure of a secret is a criminal offence. This shall be noted in the case file being inspected, and shall be accompanied by the signature of the person warned. (7) Inspection of the case file shall be authorised and enabled by the body conducting the proceedings, unless otherwise provided by the present Act. After the conclusion of the proceedings, inspection of the case file shall be authorised by the president of the court or an official person designated by him. (8) Any person having a justified interest therein may be allowed inspection of the case file in accordance with law.

Defendant may read the protocol/minutes (e.g. protocol/minutes on the taking of evidentiary action such as search of a mobile phone) [157] and place objections. [158] Defendant may appeal the

---

Article 184: (1) The parties shall have the right to inspect the case file. (2) The victim, injured party and their proxies shall have the right to inspect the case file. If prior inspection of the case file would influence the testimony of the victim or the injured party, they shall have the right to inspect the case file only after they have been examined. (3) The injured party as prosecutor shall have the right to inspect the case file after receipt of the notification referred to in Article 55, paragraph 1, of the present Act. (4) The defendant and defence counsel shall have the right to inspect the case file:1) after the defendant is interrogated, if the interrogation is conducted before the issuance of the investigation order or before service of the notice referred to in Article 213, paragraph 2, of the present Act; 2) after service of the investigation order; 3) after service of the notice referred to in Article 213, paragraph 2, of the present Act; 4) after service of private action. (5) If an urgent evidentiary action has been taken with respect to a known defendant (Article 212 of the present Act) and the conditions set forth in paragraph 4 of this Article are not met, the defendant and defence counsel shall have the right to inspect the minutes of the taking of the said action no later than 30 days from the day the said action was taken.
Article 184a: (1) Where there is a risk that the inspection of the case file or a part thereof might jeopardise the purpose of the investigation by making it impossible or more difficult to gather important evidence, or where this would jeopardise life, limb or property of considerable value, the defendant may be denied the right to inspect the case file or a part thereof for a maximum of thirty days from service of the investigation order. Where no investigation is conducted, inspection of the case file or a part thereof may be denied for the reason that this would jeopardise life, limb or property of considerable value, for a maximum of thirty days from service of the notice referred to in Article 213, paragraph 2, of the present Act. (2) The decision on the denial of the right to inspection referred to in paragraph 1 of this Article until the indictment shall be taken by the State Attorney by an order that need not be reasoned. The defendant has the right to appeal the said order within three days. The appeal shall be filed with the State Attorney who shall deliver it without delay, together with the reasons for denying the inspection of the case file, to the judge of investigation. The defendant shall not be entitled to inspect the statement of reasons of the State Attorney. The appeal of the defendant shall be decided by the judge of investigation within 48 hours. The decision of the judge of investigation to refuse the defendant's appeal shall be served on the defendant without the statement of reasons and on the State Attorney with the statement of reasons. (3) If the revealing of evidence in proceedings for especially grave forms of criminal offences set forth in Article 334, items 1 and 2, of the present Act might jeopardise the investigation in these or other proceedings conducted against the same or other defendants or would put at risk the lives of other persons, the judge of investigation may, upon the motion of the State Attorney, issue an order denying the defendant until no later than the end of the investigation inspection of certain parts of the case file containing information on the said evidence. (4) If the defendant is in investigative prison, he/she may not be denied inspection of that part of the case file which is of relevance to the assessment of the existence of grounded suspicion that he/she committed a criminal offence and of the existence of circumstances giving grounds for the decision on the imposition or extension of investigative imprisonment.
[157] Article 82: (1) A protocol shall be drawn up about every action taken in the course of proceedings concurrently with the action's taking and where this is not possible, immediately afterwards. (2) The protocol shall be drawn up by the recorder. Only in cases of search of a home or of a person or where an action is taken outside the authority's official premises and the recorder is not available may the protocol be drawn up by the person taking the action in question. (3) Where the protocol is drawn up by recorder, it shall be drawn up in such a manner that the person taking the action dictates to recorder what he/she is to enter in the protocol. (4) The person being interrogated may be permitted to state answers directly on the protocol. In the case of abuse the said person may be denied this right. Article 83: (1) The protocol shall contain the name of the government authority before which an action is taken, the location at which the said action is taken, the date and exact time when the action in question commences and ends, the names of the persons present, including in what capacity they are present, and the identification marking of the criminal case in which the action is taken. (2) The protocol must contain essential information on the course and

order deciding on the motion of parties or on exclusion of evidence (Article 86).[159] Defendant has the right to attend the evidentiary hearing and state remarks in the minutes, and to propose to the judge of investigation to ask for clarification purposes a witness or expert witness certain questions (Article 238).[160]At the trial, they are entitled to propose witnesses and expert witnesses and present evidence (Article 419, paragraph 1).

---

contents of the action taken. Only the essential contents of statements and declarations made shall be entered in the protocol in the narrative form. Questions shall be recorded in the protocol only where this is necessary for understanding the answers. Where necessary, the question asked and the answer given to it shall be entered in the protocol verbatim. If objects and documents are seized in the course of taking an action, this shall be recorded in the protocol and the seized objects shall either be attached to the protocol or their location shall be stated. (3) When taking actions such as inspection, search, temporary seizure of objects or identification, information that is important in view of the significance of such an action or for determining the identity of certain objects (description, measures and size of objects or traces, marking of objects, etc.) shall also be entered in the protocol. Where sketches, drawings, blueprints, photographs, film or other technical recordings are made, this shall also be stated in the protocol and attached to it. (4) Special provisions on the protocol shall apply to the trial protocol (Articles 409 through 412), deliberation and voting protocols (Article 88) and other protocols as prescribed by this Act.
Article 84: (1) The protocol shall be taken in an orderly manner. There may be no additions or changes to it. The parts crossed out must remain legible. (2) All changes, corrections and additions shall be entered at the end of the protocol and shall be certified by the persons signing the protocol.

[158] Article 85: (1) The person interrogated, the persons whose presence during the taking of actions in the proceedings is mandatory and, if present, the parties, defence counsel and injured person shall be entitled to read the protocol or request that it be read to them. The person taking the action shall inform them of this right. A note shall be entered in the protocol as to whether this information was given to the persons in question as well as whether the protocol was read. The protocol shall always be read if no recorder is present and a note thereon shall be entered in the protocol. (…) (7) If objections are raised concerning the contents of the protocol, these objections shall be noted in the protocol as well.

[159] Article 86: (1) Upon the motion of the parties or by virtue of his office, the judge of investigation or the president of the indictment panel shall, respectively, by the end of the investigation or after receipt of the indictment for confirmation but before its examination (Article 344, paragraph 4) issue an order excluding any unlawful evidence from the file. On the exclusion of any unlawful evidence the judge of investigation shall decide immediately and no later than three days from having learnt of the said evidence. The order deciding on the motion of the parties or on the exclusion of evidence shall be subject to special appeal. The appeal shall be decided by a higher court. (2) After the order becomes final the excluded evidence shall be enclosed in a special envelope and kept with the judge of investigation separate from the other files. They may not be inspected nor may they be used in the proceedings.

[160] Article 238: (1) Where the State Attorney makes a motion for an evidentiary hearing, he must be present at the said hearing. (2) Unless otherwise prescribed for the action taken, the defendant, subsidiary prosecutor, defence counsel and injured person may attend an evidentiary hearing. The persons present at the evidentiary hearing may state their remarks to the minutes, which shall be noted at the end of the minutes (3) Evidentiary hearing cannot be held without the defence counsel if defence is mandatory. (4) The persons participating in the evidentiary hearing may propose to the judge of investigation to ask for clarification purposes a witness or expert witness certain questions. With the permission of the judge of investigation, they may also ask questions directly. (5) If the defendant is present at an evidentiary hearing, the judge of investigation must, upon opening the evidentiary hearing, check whether he received a written instruction on his rights (Article 239, paragraph 1). If the defendant did not receive the said instruction, the judge of investigation shall proceed as stated in Article 239, paragraph 3, of this Act, and if criminal prosecution was taken over by the subsidiary prosecutor, the judge of investigation shall serve the said instruction on the defendant. (6) During the course of an evidentiary hearing the judge of investigation may

In cases of *special evidentiary measures* (e.g. interception, collection, and recording of computer data– Article 332), they may request to reproduce a recording or inspect a transcript or documents. The State Attorney shall enable the defendant immediately upon his request to reproduce a recording or inspect a transcript or documents. After the recording has been reproduced or the transcript or documents inspected, the defendant may propose at the trial that the recording, transcript or documents be reproduced or read out in full or in part (Article 332, paragraph 4).

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.*

Under Article 249 of the CPA the objects used during search of a computer and similar devices such a mobile phones shall be returned to their users after the search, provided they are not necessary for the further conduct of criminal proceedings. Personal data obtained by a search may only be used for the purposes of criminal proceedings and shall be erased without delay when this purpose ceases to exist.

In acquiring, recording, protecting and storing of data (stored in computers and devices connected thereto, as well as in devices used for collecting and transferring data, data carriers and subscription information in the possession of a service provider) under Article 263 of the CPA, special attention shall be paid to rules on the confidentiality of certain data (Articles 186 through

proceed as stipulated in Article 222, paragraph 3, of this Act (Researcher's note: may request from the relevant professional institution or an expert to be provided with the necessary explanations of certain technical or other expert issues raised concerning the evidence collected or during the taking of evidentiary actions).

188).[161] Depending on the circumstances, data that are not related to the criminal offence for which proceedings are undertaken, but which are needed by the person against whom the measure in question has been taken, may be recorded onto an appropriate medium and returned to this person also prior to the conclusion of proceedings. Any data about a child participating in the proceedings as well as any data declared secret under a special act shall represent a secret, and inspection of data that are secret shall be authorised in accordance with the provisions of the CPA and a special act (Article 183, paragraph 3-4 of the CPA. Witnesses may be questioned, e.g., on the circumstances of a search of a mobile phone/seizure of data where that is considered necessary for establishing relevant facts (e.g. where there was no formal search, but the data contained in their device were recorded by the police, then they may be questioned on the circumstances of how the police obtained their mobile device, whether they unlocked it and provided the data therein voluntarily[162]). Witnesses present during search of a home/other premises have the right to state their comments in the minutes of the search before they sign it if they deem that the search was not conducted in the manner prescribed by the CPA or that the contents of the minutes are incorrect and where necessary they may be questioned thereon during trial. Case law example: witnesses present when the police seized the defendant's mobile device in his/her home, but without a warrant, may testify on those circumstances.[163]

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.*

[161] Article 186: (1) Personal data may be collected by the competent authorities only for purposes specified by law in the framework of their tasks as laid down by the present Act. (2) Personal data may be processed only in cases specifically provided for by statute or some other regulation and only to such extent as is in line with the purpose for which the data were collected. Further processing of the said data shall be permitted only if it is not incompatible with the purposes for which the data were collected and if the competent authorities are authorised to process such data for such other purpose in accordance with the law and such processing is necessary and proportionate to that other purpose. (3) Processing of personal data concerning health or sex life shall be permitted only exceptionally if a criminal offence punishable by five years' imprisonment or a more severe penalty could not be detected or proven in any other way or where this would involve disproportionate difficulties. (4) Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade-union membership shall not be allowed (...).

[162] Supreme Court of Republic of Croatia, decision, I Kž 111/16-4, 24.2.2016.

[163] Supreme Court of the Republic of Croatia, decision, I Kž 658/15-4, 12.1.2016.

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

In addition to procedural rights specified in answer to question 55 above (including that no facts related to the victim's former sexual conduct or his/her sexual inclinations may be used as evidence in proceedings[164], and on the right to inspect the case file[165]), there is a number of provisions in the CPA intended for the specific protection of the psysical and bodily integrity of a child and victims[166], such as their right to the confidentiality of personal information; to demand

[164] Article 422, paragraph 1 of the CPA (with exceptions in paragraph 2).

[165] The victim, injured party and their proxies shall have the right to inspect the case file - if prior inspection of the case file would influence the testimony of the victim or the injured party, they shall have the right to inspect the case file only after they have been examined (Article 184). Other provisions are in references above in relation to answer to question 55.

[166] Article 43: (1) Under this Act the victim of a criminal offence shall have: 1) the right to access services providing support to victims of criminal offences; 2) the right to efficient psychological and other professional assistance and support of the body, authority or institution providing assistance to victims of criminal offences as provided for by law; 3) the right to protection from intimidation and retaliation; 4) the right to protection of the dignity of the victim when testifying; 5) the right to be heard without unjustified delay after the complaint with regard to a criminal offence has been made and to be further heard only insofar as this is necessary for the purposes of the criminal proceeding; 6) the right to be accompanied by a person enjoying his/her confidence when taking part in any acts; 7) the right to be subject to a minimum number of medical interventions and only where strictly necessary for the purposes of the criminal proceedings; 8) the right to file a motion for prosecution and a private action pursuant to the provisions of the Criminal Act, the right to participate in the criminal proceeding as an injured party, the right to be informed of the dismissal of the criminal complaint (Article 206, paragraph 3, of this Act) and of the State Attorney dropping the criminal charge, and the right to take over criminal prosecution in lieu of the State Attorney; 9) the right to be informed by the State Attorney of the acts performed as a result of his/her complaint (Article 206a of this Act) and the right to complain to a senior State Attorney (Article 206b of this Act); 10) the right to be informed without unjustified delay, at his/her request, of the release from custody or the investigative prison, the defendant having fled or the convicted person having been released, and of the measures taken for the purposes of his/her protection; 11) the right to be informed, at his/her request, of any decision finally terminating a criminal proceeding; 12) any other rights provided for by law. (2) Where the victim of a criminal offence punishable by imprisonment for more than five years has suffered severe harm as a result of a criminal offence, he/she is entitled to the professional assistance of an advisor appointed at government expense when bringing a civil claim. (3) The victim of an intentional crime of violence is entitled under a special act to compensation from the state budget. If the victim has won a civil claim, the amount awarded shall be taken into account when determining the amount of compensation. If the victim has already been awarded state compensation, the court shall act likewise when determining the amount to be awarded on the basis of the civil claim made. (4) Already at the time of performing the first act in which the victim takes part, the court, the State Attorney's office, the investigators and the police shall advise the victim in a manner he/she understands of: 1) the rights referred to in paragraphs 1, 2 and 3 of this Article and Article 44 of this Act; 2) his/her rights as an injured party. (5) The bodies referred to in paragraph 4 of this Article shall treat the victim in a considerate manner and shall make sure that he/she has understood the information given to him/her about his/her rights. (6) The bodies referred to in paragraph 4 of this Article shall instruct the victim in a manner he/she understands on what it means to participate in a proceeding as the injured party. The instruction given and the statement by the victim on whether he/she wants to take part in the proceeding as the injured party shall be entered on the record. (7) The rights referred to in paragraph 1, points 8, 9 and 11, of this Article shall also be enjoyed by legal persons against which a criminal offence was committed. The provisions of this Act governing the exercise of the said rights by the victim of a criminal offence shall apply accordingly to legal persons against which a criminal offence was committed.

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

that the hearing be closed to the public; to refuse to answer any strictly private questions not related to the criminal offence (victims with specific protection needs, victims of the criminal

---

Article 43a: (1) Before questioning the victim, the body conducting the questioning shall carry out, in cooperation with the bodies, organisations or institutions providing assistance and support to victims of criminal offences, an individual assessment of the victim. The individual assessment shall include establishing whether there is a need to take special protection measures in respect of the victim and if yes, which ones (special method of questioning the victim, use of communication technology so as to avoid visual contact between the victim and the perpetrator and other measures provided for by law). Where the victim of a criminal offence is a child, it shall be presumed that special protection measures need to be taken and it shall be established which ones. (2) The individual assessment of a victim shall take into account the personal characteristics of the victim, the type or nature of the criminal offences and the circumstances of the criminal offence. In this context particular attention shall be paid to victims who have suffered considerable harm due to the severity of the criminal offence, victims of a criminal offence committed with a bias related to their personal characteristics and victims whose relationship to the perpetrator makes them particularly vulnerable. (3) In terms of paragraph 2 of this Article, in particular victims of terrorism, organised crime, human trafficking, gender-based violence, violence in a close relationship, sexual violence and exploitation, hate crime and victims with disabilities shall be duly included in the individual assessment. (4) Individual assessments of victims shall be carried out with the involvement of the victim and shall take into account their wishes including where they do not wish to benefit from special protection measures as provided for by law. (5) The body conducting the proceeding shall keep the questioning of victims with specific protection needs to a minimum. The State Attorney may propose that such witnesses testify at the evidentiary hearing. (6) Subject to prior consent of the minister responsible for internal affairs, the minister responsible for the judiciary shall adopt an ordinance regulating the manner in which the individual assessment of a victim referred to in paragraph 1 of this Article is to be carried out. Researcher's note: the related act adopted is: *Ordinance on manner of implementation of individual assessment of the victim* (Official Gazette no. 106/17).

Article 44: (1) In addition to the rights enjoyed by the victim under this Article and the other provisions of this Act, a child victim of a criminal offence shall have the right to: 1) an attorney-in-fact appointed at government expense; 2) the confidentiality of personal information; 3) the exclusion of the public. (2) The court, the State Attorney's office, the investigators and the police shall treat the child victim of a criminal offence with special consideration, taking into account his/her age, personality and other circumstances so as to avoid any adverse effects on its upbringing and development. In taking any action in respect of the child victim the competent authorities shall primarily keep in mind the best interests of the child. (3) Where the age of the victim is unknown and it is probable that the victim has not yet turned eighteen, it shall be presumed that the victim is a child. (4) In addition to the rights enjoyed by the victim under Article 43 of this Act, victims of the criminal offence against sexual freedom and victims of the criminal offence of human trafficking have the right: 1) before being questioned, to counselling services at government expense; 2) to an attorney-in-fact appointed at government expense; 3) to be questioned at the police and the State Attorney's by a person of the same sex and that in case of any further questioning he/she be questioned, where possible, by that same person; 4) to refuse to answer any strictly private questions not related to the criminal offence; 5) to demand to be questioned via an audio-video link (Article 292, paragraph 4, of this Act); 6) to the confidentiality of personal information; 7) to demand that the hearing be closed to the public. (5) In addition to the rights enjoyed by the victim under Article 43 of this Act, a victim with specific protection needs as provided for in Article 43a of this Act shall have the right to: 1) before being questioned, to counselling services at government expense; 2) to be questioned at the police and the State Attorney's by a person of the same sex and that in case of any further questioning he/she be questioned, where possible, by that same person; 3) to refuse to answer any strictly private questions not related to the criminal offence; 4) to demand to be questioned via an audio-video link (Article 292, paragraph 4, of this Act); 5) to the confidentiality of personal information; 6) to demand that the hearing be closed to the public.

offence against sexual freedom and victims of the criminal offence of human trafficking, children victims). When reproducing a recording, if the recording includes footage of a child, the recording shall be reproduced by modifying the image and the voice of the child where this is required for the purpose of protecting the interests of the child. In doing so, account shall be taken of the interests of the proceedings as a whole (Article 330, paragraph 3 of the CPA).

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.

Acessing data stored in the Cloud

If an application also stores data on a local memory of the mobile device, such data remain and could be seized during the search.

In case of applications storing data exclusively on the online server, country of the seat of the server needs to be established and then mutual legal assistance mechanisms used.

Access to data stored in the cloud may be provided voluntarily.

According to the 2017 Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" – Report on Croatia:

> "The fact is that offenders who sexually abuse children via the internet are increasingly 'hidden' as they are making greater use of on-line 'Cloud' storage to store illegal content. This has made it more difficult to detect offenders and to provide evidence of criminal liability in criminal proceedings. In cases where the suspect is willing to cooperate or there are other sources of information concerning usernames and passwords, a court order to search his/hers accounts for such services, with aim of gathering and registering the content, is obtained. Furthermore, in some cases Croatia sends a preservation request to the owner of the service asking that they keep illegal content on the suspect's account until Croatia provides a request for international legal assistance."[167]

[167] Council of the European Union, Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime"- Report on Croatia, 5250/1/17, REV 1 DCL 1, GENVAL3 CYBER9, 11.4. 2017, https://data.consilium.europa.eu/doc/document/ST-5250-2017-REV-1-DCL-1/en/pdf, p. 63.

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

Relevant domestic legislation in international cooperation

Relevant domestic legislation in international cooperation includes the *Act on Mutual Legal Assistance in Criminal Matters* (Official Gazette no. 178/04) and the *Act on Judicial Cooperation in Criminal Matters with the Member States of the EU* (Official Gazette no. 91/10, 81/13, 124/13, 26/15, 102/17, 68/18 and 70/19).

The Act on Judicial Cooperation in Criminal Matters with the Member States of the EU, as last amended in 2019, regulates judicial cooperation in criminal matters between domestic competent judicial bodies with the competent judicial bodies of other EU Member States, which relates to:
1. European arrest warrant and surrender procedure,
2. European investigation order,
3. property freezing order,
4. recognition and execution of decisions on confiscation of property or objects,
5. recognition and execution of decisions on fines,
6. recognition and execution of sentences imposing a prison sentence or a measure involving deprivation of liberty,
7. recognition and execution of judgments and decisions imposing probation measures and alternative sanctions,
8. recognition and enforcement of decisions on precautionary measures,
9. European protection order.

In addition to Directive 2014/41/EU of the European Parliament and of the Council of 3 April 2014 regarding the European Investigation Order in criminal matters (OJ L 130, 1.5.2014), this Act transposes the following EU acts into Croatian legislation:
- Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18.7.2002),
- Council Framework Decision 2003/577/JHA of 22 July 2003 on the execution in the European Union of orders freezing property or evidence (OJ L 196, 2.8.2003),
- Council Framework Decision 2005/214/JHA of 24 February 2004 on the application of the principle of mutual recognition to financial penalties (OJ L 76, 22.3.2005),
- Council Framework Decision 2006/783 / JHA of 6 October 2006 on the application of the principle of mutual recognition to confiscation orders (OJ L 328, 24.11.2008),
- Council Framework Decision 2008/909/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments in criminal matters imposing custodial sentences or measures involving deprivation of liberty for the purpose of their enforcement in the European Union (OJ L 81, 27. 11. 2008),
- Council Framework Decision 2008/947/JHA of 27 November 2008 on the application of the principle of mutual recognition to judgments and probation decisions with a view to the supervision of probation measures and alternative sanctions (OJ L 337, 27.11.2008),
- Council Framework Decision 2009/299/JHA of 26 February 2009 amending Framework Decisions 2002/584/JHA, 2005/214/JHA, 2006/783/JHA, 2008/909/JHA and 2008/947/JHA, thereby enhancing the procedural rights of persons and fostering the application of the principle of mutual recognition to decisions rendered in the absence of the person concerned at the trial (OJ 2009 L 81, 26.3.2009),

- Council Decision 2002/187 / JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime (OJ L 63, 6.3.2002), as last amended by Council Decision 2009/426/JHA of 16 December 2008 on the strengthening of Eurojust (OJ L 138, 4.6.2009),
- Council Framework Decision 2009/829/JHA of 23 October 2009 on the application, between Member States of the European Union, of the principle of mutual recognition to decisions on supervision measures as an alternative to provisional detention (OJ L 294, 11.11.2009),
- Directive 2012/13/EU of the European Parliament and of the Council of 22 May 2012 on the right to information in criminal proceedings (OJ L 142, 1.6.2012),
- Directive 2011/99/EU of the European Parliament and of the Council of 13 December 2011 on the European protection order (OJ L 338, 21.12.2011),
- Directive 2013/48/EU of the European Parliament and of the Council of 22 October 2013 on the right of access to a lawyer in criminal proceedings and in European arrest warrant proceedings, and on the right to have a third party informed upon deprivation of liberty and to communicate with third persons and with consular authorities while deprived of liberty (OJ L 294, 6.11.2013),
- Council Framework Decision of 13 June 2002 on joint investigation teams (2002/465 /JHA), (OJ L 162, 20.6.2002),
- Council Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings (OJ L 328, 15.12.2009),
- Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA (OJ L 88/6, 31. 3. 2017),
- Directive (EU) 2016/800 of the European Parliament and of the Council of 11 May 2016 on procedural safeguards for children who are suspects or accused persons in criminal proceedings (OJ L 132, 21.5.2016),
- Directive (EU) 2016/1919 of the European Parliament and of the Council of 26 October 2016 on legal aid for suspects and accused persons in criminal proceedings and for requested persons in European arrest warrant proceedings (OJ L 297, 4.11.2016).

Suggestion: detailed information, in particular on relevant practice and case law, might be obtained at the State Attorney's Office of the Republic of Croatia.

Private-public partnership

According to Ministry of Interior's Report for 2019, during 2018 a total of 209 requests were processed from various organizational units of the police (Ministry of the Interior) for the cross-border acquisition of electronic evidence from various Internet service providers operating outside of the Republic of Croatia.[168]

According to the 2017 Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" – Report on Croatia:

[168] Ministry of the Interior, Report on work for 2019 (title in original language: Izvješće o radu za 2019. godinu), https://mup.gov.hr/UserDocsImages/dokumenti/2019/STUDENI/Godisnje%20izvjesce%20o%20radu%20Ministarstva%20unutarnjih%20poslova.pdf, p. 59.

> "In some cases, police officers use the services which some providers of electronic services provide to the police authorities to communicate and to ensure a faster and more effective response to, for example, the exploitation of children for pornography (e.g. Facebook, Skype, and Instagram Law Enforcement Response Team). International police co-operation with the police authorities in some countries (e.g. United States, Australia, New Zealand, etc.) has also been very successful in cases involving sexual abuse and exploitation of children."[169]

Available data on Government requests for customer data from foreign ISP's such as Facebook, Google, etc. can be found in transparency reports from internet service providers.[170]

Some data is also available in the recent Cybercrime Convention Committee report: The Budapest Convention on Cybercrime: benefits and impact in practice.[171]

Suggestions:

detailed and up-to-date information should be available at the Ministry of Interior - police, in particular the *Cyber Security Service/Department* ("Služba kibernetičke sigurnosti"). Namely, according to the 2019 Report on work of the Ministry of Interior that service acts as: "national contact point for: urgent exchange of data on cyber attacks under the Information Systems Attack Directive (EU); exchanging cybercrime data and sending and receiving requests for data retention for the purpose of submitting requests for international legal assistance; cybercrime for INTERPOL member states; obtaining subscriber and traffic data from internet content providers (Facebook, Twitter, PayPal ...) in order to establish the identity of perpetrators of criminal offenses for all forms of crime and all organizational units of the Ministry of the Interior" (emphasis added).[172]

---

[169] Council of the European Union, Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime"- Report on Croatia, 5250/1/17, REV 1 DCL 1, GENVAL3 CYBER9, 11.4. 2017, https://data.consilium.europa.eu/doc/document/ST-5250-2017-REV-1-DCL-1/en/pdf, p. 86.

[170] E.g. Facebook: https://govtrequests.facebook.com/about/# Google https://www.google.com/transparencyreport/; Microsoft https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report; Apple http://www.apple.com/privacy/transparency-reports/.

[171] See Requests for account information received/disclosed by Facebook, Google/YouTube and Microsoft/Skype, in: Cybercrime Convention Committee (T-CY), The Budapest Convention on Cybercrime: benefits and impact in practice, T-CY (2020)16, Strasbourg, 13 July 2020, https://rm.coe.int/t-cy-2020-16-bc-benefits-rep-provisional/16809ef6ac, p. 23.

[172] Ministry of the Interior, Report on work for 2019 (title in original language: Izvješće o radu za 2019. godinu), https://mup.gov.hr/UserDocsImages/dokumenti/2019/STUDENI/Godisnje%20izvjesce%20o%20radu%20Ministarstva%20unutarnjih%20poslova.pdf, p. 59.

Also, it is suggested to consult:

listed contact points under Article 35 of the Cybercrime Convention[173], competent authorities and channels for MLA[174], as well as departments (and persons/titles) interviewed/met (on-site visit) for the purposes of the 2017 Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime" - Report on Croatia.[175]

[173] The Ministry of Interior, General Police Directorate, Criminal Police Directorate, National Police Office for Suppression of Corruption and Organised Crime, Department for Economic Crime and Corruption, Ilica 335, Zagreb. Council of Europe, Octopus Cybercrime Community, Croatia - Cybercrime legislation, version 14.5.2020, https://rm.coe.int/octocom-legal-profile-croatia-reviewed/16809e6acf, pp. 99-100.

[174] Competent authorities and channels: For Extradition and MLA: the Ministry of Justice, Ulica grada Vukovara 49, 10 000 Zagreb. For 24/7 Contact point: Ministry of Interior, General Police Directorate, Crime Intelligence Sector, Cyber Security Department,
https://www.coe.int/en/web/octopus/-/croatia?redirect=https://www.coe.int/en/web/octopus/country-wiki?p_p_id=101_INSTANCE_AZnxfNT8Y3Zl&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-4&p_p_col_pos=1&p_p_col_count=2, last updated: 14.5.2020.

[175] Council of the European Union, Evaluation report on the seventh round of mutual evaluations "The practical implementation and operation of European policies on prevention and combating cybercrime"- Report on Croatia, 5250/1/17, REV 1 DCL 1, GENVAL3 CYBER9, 11.4. 2017, https://data.consilium.europa.eu/doc/document/ST-5250-2017-REV-1-DCL-1/en/pdf, pp. 116-120.