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

IMPORTANT TO READ BEFORE ANSWERING THE QUESTIONNAIRE:

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

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

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

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

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

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

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

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

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

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

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

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

Introductory questions:

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

Answer: University of Wrocław, research assistant; Wrocław Bar, barrister

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

Answer: Wrocław, Poland.

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

Answer: There is no legal definition of a "mobile device".

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?*

There are three ways of gaining access to the data contained in the mobile device without seizing it. The choice depends on:

1) whether the criminal proceedings have already been initiated and the search is to be conducted as an evidentiary procedure in the proceedings (then it is possible under art. 236a C.C.P.[1] [search of IT systems] or art. 237 and art. 241 C.C.P. [the interception of conversations, known also as procedural wire-tapping]) OR the search may be conducted outside criminal proceedings (not as an evidentiary procedure but rather as an intelligence operation of the Police or secret services) which is also possible if the criminal proceedings is already on – but the act itself happens regardless (art. 19 of the Police Act of April 6th 1990, t.j. Dz.U. 2020.360 – "operational control", non-procedural wire-tapping);
2) the type of the data the authorities want to acquire – under art. 237 and art. 241 C.C.P. it is only possible to gain access to "the contents of other (then telephone) conversations or communications, including e-mail correspondence, performed with the use of technical means" (art. 241 C.C.P.). During operational control by the Police or other services you

[1] Act of 6th June 1997 – Code of Criminal Proceedings, t.j. Dz.U. 2020, poz. 30; hereinafter: C.C.P.

might gain access not only to the correspondence but to the data contained in data carriers, telecommunications terminal equipment, IT systems or communication and information systems. Under art. 236a C.C.P. all the provisions concerning seizure and search apply accordingly to the administrator and user of a device that contains informatic data or of a computer system with respect to that data stored in such device or system or in a data carrier being in his disposition or usage, including electronic correspondence. It is unclear whether it is allowed to search the cloud under art. 236a – see more hereinbelow in points 13 and 26. It is certain that it is allowed under art. 19 of the Police Act.

It also has to be noted that – apart from the Police Act – there are other acts on certain secret services entitled to conduct operational control. These acts include provisions similar to art. 19 of the Police Act (namely: art. 9e of the Act of 12th October 1990 on the Border Forces; art. 118 of the Act of 16th November 2016 on the National Fiscal Administration; art. 31 of the Act of 24th August 2011 on the Military Police and military forces of law and order; art. 27 of the Act of 24th May 2002 on the Agency of Internal Security and the Intelligence Agency; art. 31 of the Act of 9th June 2006 on the Service of Military Counterintelligence and the Service of Military Intelligence; art. 17 of the Act of 9th June 2006 on the Central Anticorruption Bureau). Hereinbelow I will only refer to the Police Act since the construction of all these acts is the same.

It also needs to be underlined that an equivalent of operational control, the scope of which is identical to that of art. 19 of the Police Act, may be ordered under art. 9 of the Act of 10th July 2016 on counterterrorist actions by the Chief of the Agency of Internal Security **without court's order** towards a foreigner regarding whom there are concerns about possible terrorist activity for the period not exceeding 3 months.

Lastly, art. 218 C.C.P. constitutes the legal basis for the interception if "other communication data", namely phone records and BTS data but not the information content. Such data is handed over on the sole basis of the prosecutor's or court's order. Similarly, the Police act provides in art. 20c that the Police is entitled to obtain communication and

traffic data from service providers without neither consent nor knowledge of the interested person. Such data do not include the contents of the correspondence.

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

There are no limits regarding privacy. It is underlined in the legal doctrine that the search may not violate separate provisions on legally protected privileges, e.g. attorney-client privilege or confessional seal[2].

The search of an IT system or device under art. 236a may be ordered in any criminal case. There are also no limits as to the objective and subjective scope of the search. On the other hand, procedural wire-tapping and operational control by the Police can only be applied if the case relates to one of the most serious crimes, enlisted in the catalogue contained in art. 237 § 3 C.C.P. or art. 19 section 1 of the Police Act respectively. These catalogues are not identical. The translations of the catalogues are included in the end of the answer to this question. The Constitutional Tribunal in the judgment of 30th July 2014, K 23/11, indicated that the order of the court shall precise the technical methods to be used. However, necessary statutory amendments were not introduced and in practice the orders are not always as precise as they should be and usually only indicate a general type of control (e.g. control of messages sent by social media). Procedural wire-tapping has also limited personal (subjective) scope, i.e. it may only be applied towards a suspected person, a defendant, a victim or other person whom the defendant may contact or who may be linked to a perpetrator or an impending offence (art. 237 § 4 C.C.P.).

[2] Stefański R.A., Zabłocki S., Art. 236(a) in: *Kodeks postępowania karnego. Tom II. Komentarz do art. 167-296*, Warsaw 2019.

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

There are temporal limits to procedural wire-tapping and operational control. In criminal proceedings the interception might be ordered for 3 months with one possible extension of another 3 months (art. 238 § 1 C.C.P.). Under the Police Act the control might be order for 3 months, with a possible extension of 3 months but then, in particularly justified situations where new significant circumstances occurred other extensions for fixed term might apply for another 12 months, which makes **18 months in total** (art. 19 section 8 and 9 of the Police Act)**.**

The catalogue of art. 237 § 3 C.C.P. is as follows:

1) homicide;

2) exposure to common danger or bringing a catastrophe;

3) trafficking;

4) kidnapping;

5) forcing a ransom;

6) aircraft or watercraft hijacking;

7) armed robbery, robbery or extortion;

8) an attack on the independence or integrity of the state;

9) an attack on the constitutional system of the state or its supreme organs, or on a unit of the Armed Forces of the Republic of Poland;

10) espionage or disclosure of classified information classified as "secret" or "top secret";

11) collecting weapons, explosives or radioactive materials;

12) forgery and trade in counterfeit money, payment instruments or negotiable documents entitling to receive a sum of money, goods, cargo or material prize or containing an obligation to pay capital, interest, share in profits or a declaration of participation in the company;

12a) counterfeit of invoices or the use of forged or altered invoices insofar as it may be relevant for determining the amount of tax payable or its return, and the issuing and use of invoices confirming false facts as to the factual circumstances that may be relevant for determining the amount of tax payable or its refund or refund of other public liabilities;

13) manufacturing, processing, trading and smuggling of narcotic drugs, precursors, substitutes or psychotropic substances;

14) being a member of an organized criminal group;

15) any crime concerning property of significant value, which is more than 200.000 PLN (about 48.000 EUR)

16) use of violence or unlawful threats in connection with criminal proceedings;

16a) giving false testimony or presenting a false expert opinion or translation by an expert or translator;

16b) false accusation of another person of committing a crime or a tax offense;

16c) creating false evidence or conducting other deceptive actions aimed at directing the prosecution of a crime or a tax offense against another person, or taking such measures in the course of the proceedings;

16d) concealing evidence of innocence of a person suspected of committing a crime or a tax offense,

16e) notifying the Police or the prosecutor of an unfulfilled crime or a fiscal crime;

16f) aiding and abetting;

16g) failure to notify about the crime when there is legal duty to do so;

17) bribery and paid protection;

18) pimping;

19) crimes specified in Chapter XVI of the Act of 6 June 1997 - Penal Code (Journal of Laws of 2019, items 1950 and 2128) and in art. 5-8 of the Rome Statute of the International Criminal Court, drawn up in Rome on July 17, 1998 (Journal of Laws of 2003, item 708 and of 2018, item 1753).

The catalogue in art. 19 section 1 of the Police Act contains crimes:

1) against life, provided for in art. 148-150 of the Criminal Code,

2) provided for in art. 134, art. 135 § 1, art. 136 § 1, art. 156 § 1 i 3, art. 163 § 1 i 3, art. 164 § 1, art. 165 § 1 i 3, art. 166, art. 167, art. 173 § 1 i 3, art. 189, art. 189a, art. 211a, art. 223, art. 228 § 1 i 3-5, art. 229 § 1 i 3-5, art. 230 § 1, art. 230a § 1, art. 231 § 2, art. 232, art. 233 § 1,

1a, 4 i 6, art. 234, art. 235, art. 236 § 1, art. 238, art. 239 § 1, art. 240 § 1, art. 245, art. 246, art. 252 § 1-3, art. 258, art. 269, art. 270a § 1 i 2, art. 271a § 1 i 2, art. 277a § 1, art. 280-282, art. 285 § 1, art. 286 § 1, art. 296 § 1-3, art. 296a § 1, 2 i 4, art. 299 § 1-6 and art. 310 § 1, 2 i 4 of the Criminal Code,

2a) provided for in w art. 46 section 1, 2 i 4, art. 47 oraz art. 48 section 1 i 2 of the Sports Act of 25th July 2010 (Dz. U. 2019.1468, 1495 and 2251),

2b) provided for in art. 178-183 Act of 29th July 2005 r. on the trade in financial instruments (Dz. U. 2018.2286, 2243 and 2244) oraz art. 99-100 Act of 29th July 2005 r. on the public offers and the rules of introducing financial instruments into organised trade systems and on public limited companies (Dz. U. 2019.623, 1655, 1798 and 2217),

3) against business trading, provided for in art. 296-306 of the Criminal Code, causing damage or directed against property, if the damage or the value of the property exceeds the amount equal to 50 minimum salaries provided for in separate provisions,

3a) against sexual freedom and decency, when the victim is underage or if the pornography mentioned in art. 202 of the Criminal Code involves a person who is underage,

3b) provided for in chapter 11 of the Act of 23rd July 2003 on the protection of monuments and care over the monuments (Dz. U.2018.2067 and 2245 and Dz.U.2019.730 and 1696), in chapter 5 Act of 14th July 1983 on the national archives (Dz. U. 2019.553, 730 and 2020), in chapter 5a Act of 21st November 1996 o museums (Dz. U. 2019.917 and 1726), in chapter 11a of the Act of 27th June 1997 on libraries (Dz.U. 2019.1479) and in chapter 6 Act of 25th May 2017 on the restitution of national cultural goods (Dz. U. 2019.1591),

4) tax crimes, if they concerned the amount or lowered the taxes by more than 50 minimum salaries provided for in separate provisions,

4a) tax crimes provided for in art. 107 § 1 of the Fiscal Penal Code,

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

5) illegal production, possession or trading in weapons, ammunition, explosive material, narcotic drugs, precursors, psychotropic substances, nuclear or radioactive materials,

6) provided for in art. 8 of the Act of 6th June 1997 – Introductory provisions to the Criminal Code (Dz. U. 554 i 1083, Dz.U. 1998.715, Dz.U.2009.1149 and 1589 and Dz.U.2010.626),

7) provided for in art. 43-46 of the Act of 1st July 2005 on procurement, storage and transplantation of cells, tissues and organs (Dz. U. 2019.1405),

8) indictable under international conventions ratified by the statute, provided for in polich criminal acts,

9) provided for in points 1-8 hereinabove or mentioned in art. 45 § 2 of the Criminal Code or in art. 33 § 2 of the Fiscal Penal Code (relating to the property of significant value which under C.C. means more than 200.000 PLN) – in order to find property subject to confiscation because of these crimes.

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

Yes, under art. 241 C.C.P. or art. 19 of the Police Act. If the court ordered controlling certain data by certain means, the authorities executing the order (Police or intelligence services) are entitled to conduct any effective actions that stay within the limit of the order. The law does not limit technical means that may be ordered in order not to exclude new technologies that might occur.

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

It may be copied.

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

No.

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

The questions seems more relevant to the case of seizure of the device. See answer to point 20 below.

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

In general the person who is the owner/disponent of a searched place [computer system] shall be informed of the search. That is due to the fact that such decision is subject to interlocutory appeal which may be filed by a person whose rights were infringed (art. 236 § 1 C.C.P.) and all decisions issued outside the courtroom that are subject to interlocutory appeal have to be delivered to all entities entitled to file it (art. 100 § 4 C.C.P.). So, the information comes as a delivery of the prosecutor's or judge's order of seizure and/or search which is handed over at the beginning of the procedure. It is doubtful whether the delivery of the court's order of the search of an IT system may be postponed under art. 218 C.C.P. for the fixed time. It would serve the efficiency of conducted actions since the data are easily erased from the system. However, the first stage of any search is a request of voluntarily handing over things (data) looked for (art. 224 § 1 C.C.P.) which could not be formulated if the delivery of the search warrant was postponed.

In case of procedural wire-tapping under art. 237 and art. 241 C.C.P. the court's order is subject to interlocutory appeal under art. 240 C.C.P but the delivery of such order may be postponed as long as it necessary for the sake of proceedings but in preparatory proceedings no longer than until the conclusion.

However, if the action is conducted under art. 19 of the Police Act, the court's order is never delivered to the interested person. If the control results in criminal proceedings, he or she will get to know about the fact that his or her data were controlled from the criminal case file. If no criminal proceedings against such person was initiated, he or she would never become aware of this fact. Polish law does not fulfil conventional and constitutional standard in this respect, which was twice pointed out by the Constitutional Tribunal (judgment of 30th July 2014, K 23/11; judgment of 25th January 2006, S 2/06) but so far no statutory changes were introduced.

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

a) A search of an IT system under art. 236a C.C.P. might be ordered by the court or the prosecutor whenever there is reasonable suspicion that the data therein contained might be relevant for the ongoing case.

b) Procedural wire-tapping in criminal proceedings may only be ordered by the court ruling on the prosecutor's motion (art. 237 § 1 C.C.P.). In case of great urgency the prosecutor may order controlling which starts immediately, but he or she is obliged to apply for the court's approval within 3 days. The court adjudicates within 5 five days. If the prosecutor's decision is not approved, all gathered data is immediately erased (art. 237 § 2 C.C.P.).

c) Operational control under the Police Act may only be ordered by the District Court ruling on the motion of the Chief Constable, Chief of the Police Central Bureau of Investigation, Chief of the Police Internal Affair Bureau approved by the Attorney General, or on the motion of the Provincial Police Chief approved by the District Attorney. The motion may only be granted if the requirements of the subsidiarity principle are fulfilled – art. 19 section 1 of the Police Act provides that the control is only possible if other means were proven ineffective or would be useless.

The decision always comes in a form of order (pol. *postanowienie*).

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

Yes – see the answer to question 20. Apart from the difference concerning the existence of duty to unlock the device, the only other difference consists in the fact that – as it has already been mentioned - procedural wire-tapping may only be applied towards a suspected person, a defendant, a victim or other person whom the defendant may contact or who may be linked to a perpetrator or an impending offence (art. 237 § 4 C.C.P.). There are no differences in the position of a witness, victim or another party in other elements of procedure.

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.*

There are no specific regulations addressing the issue. It has lately been the subject of interest of the legal doctrine and there are first judicial rulings. The views are divergent when it comes to determine whether it is legal to search the cloud and what should be the legal grounds for it. On one hand, it is argued that gaining access to the data stored in the computing cloud is not

possible under art. 236a C.C.P. (search of mobile device) if the data contains the merits of the document, not metadata, because such action is more similar to the wire-tapping than to the retention of the data[3]. In that interpretation art. 236a allows access to the information on the date of the e-mail, sender, received but not to the contents of the message itself if the data is not saved on the device itself but in the cloud. A procedural wire-tapping must therefore be ordered by the court which is only possible in proceedings concerning most serious crimes specified in art. 237 § 3 C.C.P. However, there is also the second view according to which the difference between art. 236a and art. 237 C.C.P. consists in the static or dynamic character of the actions taken – whereas art. 236a C.C.P. allows to search the cloud with regard to already existing data, art. 237 C.C.P. aims at monitoring current activity[4]. This interpretation seems more adequate to the wording of art. 236a C.C.P., since it expressly mentions "electronic correspondence" as its subject-matter.

It is also clear that acquiring data from the cloud would be possible under art. 19 of the Police Act.

Regardless of the legal basis, under art. 237 C.C.P. and art. 19 of the Police Act the order has to be delivered to the entity who administers the system, so the international instruments mentioned seem the only option. However, art. 236a applies both to the administrator and **user** of the system who obviously has access to the data. If we accept the view that you may access the contents of the files under art. 236a, it seems enough to deliver the order to the user.

This regulation is heavily criticised in the doctrine due to its ambiguity, imprecise divisions between different evidence procedures and ineffectiveness as well as lack of procedural

[3] Kudła J., Staszak A., *Controlling correspondence stored in the cloud during and outside criminal proceedings (pol. Procesowa i operacyjna kontrola korespondencji przechowywanej w tzw. Chmurze*), Prokuratura i Prawo 2017, no. 7-8, pp. 31-57, and the judgment cited therein of the District Court in Zielona Góra of 6th March 2017, II Kp 123/17, LEX nr 2355988.

[4] K. Kremens, in: ed. J. Skorupka, *Model dopuszczalnej ingerencji w prawa i wolności jednostki w procesie karnym. The Model of Acceptable Interference with the Rights and Freedoms of an Individual in the Criminal Process*, Warsaw 2019, pp. 260-264, 287-293, 602-606, 629-635.

safeguards[5]. There is no case law resolving the issue so at the moment it is really hard to tell which option will prevail.

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

Yes, as it has been stated, procedural wire-tapping and operational control are only admissible in case of most serious crimes specified in art. 237 § 3 C.C.P. and art. 19 section 1 of the Police Act. See the catalogues in point 5 above. However, search of IT system under art. 236a may be conducted in any criminal proceedings.

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

The issue of exclusionary rules is very problematic in Poland. As of 15th March 2016, controversial art. 168a, art. 168b and art. 237b C.C.P. are in force, which are heavily criticized in the legal doctrine and were subject to several judicial rulings, including those of the Supreme Court, trying to establish an interpretation that would allow their application without breaching constitutional and conventional standards of fair trial.

Art. 168a C.C.P. provides that an evidence must not be declared inadmissible solely for the reason of its acquisition in breach of rules of proceedings or by criminal act, unless it was acquired in connection with the duties of public servant, in consequence of: homicide, causing heavy injury or unlawful deprivation of liberty. It seems at first sight that this provision basically states that illegally obtained evidence is admissible. However, the judiciary and the legal doctrine established two other interpretations of this provision. According to the first view it is true that the evidence cannot be declared inadmissible **solely** for the reason of breaching the law in acquiring it, but if the court establishes that admitting such evidence would lead **also** to a breach of constitutional and conventional standard of fair trial, it is obliged to exclude such evidence. According to the second interpretation, due to ambiguity caused by doubtful use of punctuation in the provision, there are two separate exceptions to the prohibition of excluding

[5] *Ibidem;* A. Lach*, Przeszukanie na odległość systemu informatycznego*, Prokuratura i Prawo 2011, no. 9, pp. 67-79.

the evidence. Firstly, the evidence must be excluded if it has been acquired in connection with the duties of public servant and at the same time in breach of the rules of proceedings or by criminal act. Secondly, it must be excluded if it has been acquired in consequence of homicide, causing heavy injury or unlawful deprivation of liberty, regardless who acquired it (public servant or private person, e.g. the accused). Both views are represented in the legal doctrine and jurisprudence, sometimes in conjunction[6]. Such pro-constitutional approach leads to the conclusion that breaching the rules of acquiring any evidence in general shall lead to their inadmissibility. However, Polish jurisprudence and the legal doctrine tend to graduate infringements due to their gravity and do not present an automatic approach of excluding any evidence due to any, even minor, breach of the law. It is thus not possible to say that – even if the pro-constitutional approach described above is embraced by the court – any breach of the rules of acquiring evidence leads to its inadmissibility. Serious infringements, however, lead to its exclusion, unless a literal interpretation of the criticized art. 168a is applied.

A separate issue is that of art. 168b and art. 237b C.C.P. Those provisions were introduced on 15th April 2016 as well and relate to operational control and procedural wire-tapping. They both have almost identical wording and identical meaning. They provide that in case of so-called random discoveries, i.e. if during wire-tapping the evidence of another crime (which could but did not have to have been committed by another person and which can but does not have to belong to the statutory catalogue as long is it is belongs to the category of ex officio prosecuted offenses) than the one specified in the court order is discovered, the prosecutor decides on its use in criminal proceedings. These provisions were criticized because on literal basis it seems they put into the prosecutor's hands the decision on the admissibility of evidence gathered outside the court's order. However, it is argued that this competence only means that the prosecutor is entitled to decide whether to file an evidentiary motion for the use of such

[6] See e.g. judgment of the Supreme Court of 26th June 2019, IV KK 328/18, OSNKW 2019/8/46; judgments of the Court of Appeals in Wrocław: of 22th November 2017, II Aka 224/17, LEX no. 2464913, and of 27th April 2017, II Aka 213/16, LEX no. 2292416; K. Lipiński, *Klauzula uadekwatniająca przesłanki niedopuszczalności dowodu w postępowaniu karnym (art. 168a k.p.k.)*, Prokuratura i Prawo 2016, no. 11, pp. 44-59; Ł. Cora, *Aksjologia procesowa a dopuszczalność dowodu z art. 168a k.p.k.*, Państwo i Prawo 2018, no. 10, pp. 121-132.

evidence after issuing a decision on its use in preparatory proceedings; it is still for the court to decide whether to admit the evidence[7]. The second issue concerns the part of these provisions where it seem to be allowed to use the evidence in proceedings concerning all – even minor – crimes that are prosecuted *ex officio*, e.g. stealing a bicycle, although wire-tapping itself is only admissible in case of most serious crimes. However, the Supreme Court in the judgment of 7 judges of 28th June 2018, I KZP 4/18, OSNKW 2018/8/53, ruled that such evidence is only admissible in proceedings concerning crimes enlisted in the catalogues of crimes justifying ordering wire-tapping or operational control, i.e. in cases concerning most serious crimes, as the literal interpretation of art. 168b and art. 237a C.C.P. leads to irrational conclusions.

Mobile device seized

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

Yes, the mobile device can be seized under art. 217 C.C.P.

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

There are no separate rules of seizure of mobile devices; the general rules of seizing things for the purposes of criminal proceedings apply. These are as follows. According to art. 217 § 1 C.C.P. any person is obliged to hand over any thing that may be of evidentiary value or may secure the execution of a future fine, forfeiture, damages or other financial measures – if the judge or the prosecutor (depending on the stage of proceedings) so demands. In case of great urgency such demand may be made by the Police or other competent authority. If the seizure had been ordered by the Police, it is subject to prosecutor's or court's approval if the person who handed the thing over so demands; the approval must be delivered to this person within 14 days (art. 217 § 3 C.C.P.). It the person requested to hand over things refuses to do so, the thing may be forcefully taken or a search may be conducted (art. 217 § 5 C.C.P). There are no specific formal requirements other than the evidentiary value for the proceedings of the seized device.

[7] See R. Koper, *Podmiotowe i przedmiotowe granice stosowania podsłuchu w procesie karnym*, Ius Novum 2019, no. 1, pp. 26-44; judgment of the Court of Appeals in Warsaw of 13th June 2016, II Aka 133/16, LEX no. 2171252.

As to formal requirements of the search of a person or premises in order to acquire a mobile device, a search – according to art. 219 § 1 C.C.P. – may be conducted if there is a reasonable suspicion that the thing or person looked for is located in the searched place or possessed by the searched person. There are no requirements as to the gravity of crime that is the subject of proceedings, although some legal scholars claim that such requirements shall be derived directly from the principle of proportionality enacted in art. 31 of the Polish Constitution – limitation to human rights and freedoms must never exceed what is necessary in order to protect other constitutionally approved values. The basis of the search – once again – is the decision of the judge or the prosecutor but in case of great urgency Police may proceed without such decision (art. 220 § 1-3 C.C.P.). Such search, in contrast to *regular* seizure, must always be approved within next 7 days by the prosecutor or the judge, regardless of the interested person's demand, unless the thing was voluntarily handed over (art. 230 § 1 C.C.P.).

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

Yes. According to art. 236a C.C.P. all the provisions concerning search apply accordingly to the administrator and user of a device that contains informatic data or of a computer system with respect to that data stored in such device or system or in a data carrier being in his disposition or usage, including correspondence sent by electronic mail. This means that a mobile device or a computer system may be searched as any person or place under general conditions described in point 17. The conditions of conducting search must be fulfilled separately for the mobile device.

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

There are no statutory limits as to the scope of the search. It is underlined in the legal doctrine that the search may not violate separate provisions on legally protected privileges, e.g. attorney-

client privilege or confessional seal[8]. The search of the device may include all the data it contains. The search may be conducted in all cases concerning crimes, regardless of their gravity, although some legal scholars claim that such requirements shall be derived directly from the principle of proportionality enacted in art. 31 of the Polish Constitution – limitation to human rights and freedoms must never exceed what is necessary in order to protect other constitutionally approved values. Nevertheless there is no catalogue of crimes which justify the search. The order of search, however, shall precise what is to be found. The search in general must always be oriented to finding specific things, because it is only legal if there is reasonable suspicion that the thing (data) looked for are in particular place (device); fishing expeditions are not allowed (art. 219 § 1 C.C.P.). What is more, the first stage of any search must be calling the owner/person searched to voluntarily hand over things (data) looked for (art. 224 § 1 C.C.P.). The court's or prosecutor's order must then indicate what data is to be found during the search. Unfortunately, the general practice in any types of search is to formulate this indication in a very wide and vague way, e.g. that the search is directed at finding "any things which were acquired through committing a crime or possession of which is forbidden". Probably, that would also be the case for the search of a mobile device.

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

Yes, it is. As it was mentioned, any person receiving the order is legally obliged to hand over therein specified things and is called to do so (art. 217 § 1 and 2 C.C.P.). If he or she refuses, they may be forcefully taken (art. 217 § 5 C.C.P). Similarly, the first stage of any search (which means both searching premises in order to acquire things and searching mobile device in order to acquire data), as it has already been mentioned, consists of formulating a request for the things or data to be handed over voluntarily (art. 224 § 1 C.C.P.). Only if this request is not followed by the person in question, the search *sensu stricto* begins. So, if the data is handed over voluntarily, the search itself is not conducted. Whether the thing was voluntarily handed

[8] Stefański R.A., Zabłocki S., Art. 236(a) in: *Kodeks postępowania karnego. Tom II. Komentarz do art. 167-296*, Warsaw 2019.

over or found during search is also important in determining the obligation to deliver the prosecutor's or court's decision on approval of the search whenever it was conducted by the Police out of their own initiative in a case if great urgency. The search must always be approved within 7 days but the decision only has to be delivered to the interested person if he or she so requested (art. 220 § 3, art. 230 § 1 C.C.P.).

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

It depends on the procedural position of the owner/person in possession. If he or she is the accused, the suspect or the "suspected person" (pol. *osoba podejrzana* which means a person who has not yet formally been charged but in fact he or she is in the field of interest of the prosecution as a potential suspect – from the moment of first procedural action against him or her, e.g. beginning of search, stop or arrest), then the rule of *nemo se ipsum accusare tenetur* applies. Such person is thus not obliged to voluntarily and actively give any incriminating evidence. On the other hand, witnesses (who also include the victim) are obliged to truthfully say everything they know when interrogated which may include the information on passwords if it matters in evidentiary proceedings. Legally unjustified refusal to testify – even in part – may lead to coercive measures, such as fine and in extreme cases even arrest or detention up to 14 days (art. 285, art. 287 C.C.P.). One should also remember that usually cooperation with the Police and the prosecutor is in the best interest of the victim.

What is most interesting is that it seems there is no legal basis to force a witness to unlock the device by his or her fingerprints or face recognition technology. I am not aware of any judicial rulings on the matter as well. It might also be doubtful in case of the accused/suspect/suspected person. Freedom from self-incrimination only covers active cooperation; the accused is not obliged to actively cooperate but he is obliged to passively bear certain actions specified in art. 74 § 2 C.C.P., which include taking fingerprints. That would suggest that it is allowed to use the accused or suspect's fingerprints to unlock his or her phone. It is thus very unclear and even more when it comes to face recognition technology. I am also not aware of any jurisprudence on the matter. What is also worth underlining is that it is not

questioned in Polish legal doctrine that giving a sample of one's voice would require active cooperation of the defendant and thus cannot be forced. However, it is approved that the authorities are free to acquire such sample by contrivance, e.g. by recording the accused's voice during other procedural actions like trial.

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

In general, if the thing is seized the authorities are aware of who was in possession of this thing. The person in possession is not always the owner. If the authorities are also aware of that fact, they are obliged to deliver both to the owner and the person in possession the decision (order) on search or seizure. That is due to the fact that such decision is subject to interlocutory appeal which may be filed by a person whose rights were infringed (art. 236 § 1 C.C.P.) and all the decision issued outside the courtroom that are subject to interlocutory appeal have to be delivered to all entities entitled to file it (art. 100 § 4 C.C.P.). So, the information comes as a delivery of the prosecutor's or judge's order of seizure and/or search.

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

Yes. When the mobile device is already seized and it becomes necessary to analyse its contents, the prosecutor, the Police or the court do not analyse it by themselves but appoint an expert witness (usually an informatic or forensic expert) to extract the data and present it in a form of expert witness's opinion on the contents of the device. The expert uses the best methods according to his or her knowledge in order to acquire as much data as possible.

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

25. Yes – see the answer to question 20. Apart from the difference concerning the existence of duty to unlock the device, the only other difference consists in the fact that – as it has already been mentioned - procedural wire-tapping may only be applied towards a suspected person, a defendant, a victim or other person whom the defendant may contact or who may be linked to a perpetrator or an impending offence (art. 237 § 4 C.C.P.). There are no differences in the position of a witness, victim or another party in other elements of procedure.

26. *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.*

It is unclear and the views of legal scholars are divergent when it comes to answering the question. As it was already discussed in point 13, there is no common view whether the data stored in cloud shall be accessed in criminal proceedings via search or procedural wire-tapping. Of course the decision on this issues is of huge importance, since the search of an IT system may be ordered by the prosecutor under art. 236a C.C.P. and the wire-tapping may only be ordered by the court. Since the expert shares the view that art. 236a C.C.P. is the right legal basis for searching the cloud with respect to the data that are already stored there rathen than monitoring current activity, further considerations are based on this scenario. Art. 236a provides that an all the provisions concerning seizure and search apply accordingly to the administrator and user of a device that contains informatic data or of a computer system with respect to that data stored in such device or system or in a data carrier being in his disposition or usage, including electronic correspondence. There are no doubts that the mobile device may be searched under art. 236a C.C.P. However, as it has been fairly pointed out by A. Lach[9], the search of the cloud through the mobile device would constitute a so-called "enhanced search" – it would constitute a search of a system that is accessible through another system – the one being searched. Art. 236a C.C.P. does not provide that it is permitted. It leads to the conclusion that the requirements for the search and another decision shall be issued and delivered on the matter in the same manner as described in point 13.

Nevertheless the practice is totally different and depends solely on the technical possibilities of gaining access to the data – if the passwords are known by the expert witness or bypassed, the examination of the device simply involve the examination of the contents of the cloud. In fact,

[9] A. Lach, *Przeszukanie na odległość systemu informatycznego*, Prokuratura i Prawo 2011, no. 9, pp. 67-79.

even decisions under art. 236a on the search of the mobile device are usually not issued at all – the device seized is just handed over to the expert.

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

If the data is acquired through the search of mobile device, such circumstance makes no difference. It would only matter if the data is to be acquired from the service provider, not through the mobile device. If it is not possible to identify the service provider who is supposed the hand over the data from the cloud, it cannot in fact be executed.

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

It would only by legally possible by applying the procedure described hereinabove for any situations of non-seizure of the device, especially operational control under art. 19 of the Police Act.

29. *How is the access to data kept by a Service Provider related to the device regulated? Is it performed upon a Court order, or also through other means?*

The answer is partly given in points hereinabove. The access is regulated depending on the type of data (*traffic data* or the contents of the message/document).

When it comes to traffic data, metadata, art. 218 C.C.P states that it has to be handed over by the service provider upon the prosecutor's or court's order whenever they are significant in criminal proceedings. Such order is delivered to both service provider and user, but art. 218 § 2 C.C.P. states that its delivery may be postponed (especially in case of service user – D.C.) for a fixed term which is necessary in the light of the interests of the case, but no longer than until final ruling on merits. What is more, under art. 218a service providers are obliged to secure the data from loss for a fixed term not exceeding 90 days. Such order of securing the data shall later be followed by an order under art. 218 C.C.P. However, under art. 218a § 2 C.C.P. the data which is not important for the proceedings shall be immediately released.

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

With regard to the contents of messages or documents, as it has already been mentioned, acquiring such data from the service provider requires – according to the legal doctrine – issuing the court's order on procedural wire-tapping or operational control.

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

Yes, as it has been stated in point 5.

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

See the response in point 15 hereinabove.

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

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

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

32. **Question***: In cases where the examination or data acquisition is not possible without changing the configuration of the device, is there a strict protocol that should be followed (e.g. procedure*

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

and changes should be tested, validated, and documented)? If yes, please specify on what rules this is based and what the requirements are. Please also provide examples.

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

There is no strict protocol that should be followed. As it has already been mentioned, in general the device is examined by an expert who is entitled the use any methods necessary to extract all needed data from the device. However, he or she is supposed to follow all forensic rules that make the outcome of such examination credible. The expert witness statement has to contain among others the report of actions carried out (art. 200 § 2 point 5 C.C.P.). In an expert witness statement all the methods used have to be explained in a way which makes it possible for the court to check correctness of the procedures conducted. This means that all changes in the device shall be documented, so that if another expert is appointed in the future, he or she will be able to assess the primary state of the device. One should also bear in mind art. 207 § 2 C.C.P., providing that if during examination the thing examined might be destroyed or altered, part of the thing shall be kept in altered state if possible, and if not – its primary state shall be perpetuated otherwise.

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

Answer: There are no specific rules regulating the use of mobile forensics tools using AI technology. The catalogue of evidence that are admissible in Polish criminal proceedings is open. That means that if a new way (technology) of acquiring evidence emerges, it can be used to acquire evidence as long as it does not violate other provisions of the law, e.g. the rules on seizing electronic data or conducting electronic surveillance of private conversations. Once the data/the device is legally acquired, there are no limitations on admissible ways of analysing it, which means AI may be used.

What also needs to be underlined is that usually if a mobile device is seized, the analysis of the data is conducted by an appointed expert, usually in informatics. The expert witness may use

any methods of analysis whatsoever, as long as the final statement explains the methods and the results in a logical way.

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

Answer: Indication of length of answer: couple of paragraphs

The discussion on the matter is not very advanced; there are only a few papers on the matter and almost no judicial rulings. The main issue obviously concerns the scope of right to search data stored in the cloud and the problem of controlling the conversations run through devices registered abroad. The legal doctrine is divided as to whether it is legal to search cloud without initiating international procedures. Apart from what has already been said, there are voices that as long as the user who has access to the cloud is in Poland, it is legal to search the cloud under already discussed provisions[10]. Other scholars present the view that it may only be done *via* international legal help, since it would constitute a search conducted abroad and thus violating another state's sovereignty[11]. However, the practice indicates that such searches are conducted if the Police or other service come in possession of the password or the expert witness technically is able to access the data.

There are no separate procedures other than EIO and mutual agreements.

***35.* 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?*

[10] See M. Gabriel-Węglowski, *Działania antyterrorystyczne. Komentarz,* Warszawa 2018.
[11] P. Opitek, *Wybrane aspekty pozyskiwania dowodów cyfrowych w sprawach karnych,* Prokuratura i Prawo 2018, no. 7-8, s. 65-85; M. Siwicki, *Przetwarzanie danych informatycznych w chmurach obliczeniowych. Wybrane aspekty prawnokarne i procesowe*, Palestra 2015, no. 1–2.

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

Answer: There is no provision that regulates positive grounds that would be decisive as to whether an EIO shall be issued. Negative grounds are expressly stated in the C.C.P. The procedure of issuing an EIO is set by art. 589w – art. 589zd C.C.P. Art. 589 § 1 C.C.P. empowers the court or the prosecutor (whoever is running the case at particular stage) to issue an EIO whenever it is necessary to acquire evidence that remains or may be conducted on the territory of another EU member-state. The EIO may be issued by the Police if they conduct proceedings but it requires the prosecutor's approval. It is expressly stated in art. 589w § 4 C.C.P. that the EIO may apply to electronic surveillance of telephone or other conversations or messages. Art. 589w § 7 C.C.P. allows issuing an EIO in the course of operational activities of the Police or other similar forces (i.e. outside the scope of criminal proceedings) after agreeing with the relevant authority of another member-state the length and conditions of executing it. In these cases, the EIO must be approved by the prosecutor as well, unless the nature of the evidence requires under national law court's permission which then has to be granted. This is the case of operational control or procedural wire-tapping. Art. 589x C.C.P. forbids issuing an EIO if 1) it is not necessary in the light of interest of the justice system 2) Polish law does not allow conducting or acquiring certain evidence. Art. 589y C.C.P. regulates formal requirements of the EIO and its translation to the receiving state's language. Art. 589z C.C.P. regulates an EIO pertaining to handling a person that is deprived of liberty in another state for the purpose of evidentiary actions. Art. 589za C.C.P. provides that the Polish authority issuing the EIO may demand its representative's presence during the evidentiary action abroad. Art. 589zb precises that the EIO shall be directly delivered to a competent authority of another member state, but District Courts, District Prosecutors, Ministry of Justice, National Prosecutor or European Judicial Network may be involved. Art. 589zd C.C.P. regulates situations where procedural wire-tapping was ordered by Polish authorities against a person who remains on the territory of another member state but issuing an EIO is not necessary (e.g. such person uses a Polish telephone number). In such cases, the Police or the prosecutor notifies a relevant authority of the member state of the intention to conduct electronic surveillance or that it is or was conducted, depending on when it turns out that the person mentioned remains on the territory of this member state.

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

Answer: According to P. Opitek[12], most motions under MLAT are addressed to the US but the system has been proven ineffective due to a variety of factors:

1) the necessity of being very precise while construing the motion due to the prohibition of fishing expeditions in American law
2) difficulties in obtaining data regarding smaller offenses or offenses connected with freedom of speech due the application of *de minimis* rule and non-mandatory prosecution in American law
3) lengthy procedures (8 to 15 months).

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

Answer: With regard to Polish private telecommunication companies, handling any data is regulated by the law, as it has already been explained. I am not aware of any other practices than those provided for by the law.

There is no legal framework for cooperation in acquiring data with foreign private companies (e.g. Google, Microsoft). It has been noted in the jurisprudence that – as application of MLAT is usually ineffective – prosecutors tend to address such companies directly, invoking provisions of national law and demanding data although there is no legal framework for that and no guarantee of receiving a positive answer[13]. It has also been written that if such motion was granted, the data is used as evidence in criminal proceedings, although the National Prosecutor's Office stated in an internal document of Aug 12th 2015, no. PG V WM 0280/2/15,

[12] P. Opitek, *Wybrane aspekty pozyskiwania dowodów cyfrowych w sprawach karnych,* Prokuratura i Prawo 2018, no. 7-8, s. 65-85.
[13] *Ibidem.*

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

that acquiring data from overseas shall be strictly limited to Police cooperation and such methods shall not be used as an alternative to formal motions[14]. Poland has no executive agreement to the US CLOUD Act.

[14] *Ibidem.*

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

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

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

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

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

There are no specific rules as to the analysis of data from mobile devices.

The Law Enforcement Directive 2016/680 was implanted to national legal system by the Act of 14th December 2018 on the protection of personal data processed for the purposes of prevention and fighting criminal offences. The art. 3 of the Act excludes from its scope of application the data – including the data created or processed with the use of informatic technologies – contained in the case file in criminal proceedings. It thus may only apply to data acquired by operational control under art. 19 of the Police Act as long as it was not included in the criminal proceedings case file. However, it is pointed out by legal scholars that art. 17 of the Directive has not been implemented at all which makes the implementation improper[15].

[15] M. Kusak, P. Wiliński, *Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne,* Warszawa 2020.

Art. 19 section 8 of the Police Act provides that any data irrelevant to criminal proceedings has to be immediately and collectively destroyed which has to be officially recorded. However, in practice it often happens that private, sensitive data are transferred to the criminal case file alongside with the data that is really important in proceedings. The same applies to data gathered by evidentiary actions with the boundaries of criminal proceedings. Destroying irrelevant data is a rare exception.

The protection of the right to fair trial and non-discrimination lies mostly in the hands of the court, who is obliged to dismiss any motion to conduct evidence which it deems inadmissible in the light of the standard of fair trial – compare the answer to question 58.

Any information relevant to criminal proceedings may be retained/copied (art. 218 C.C.P.) and is kept in the case file as long as it exists. According to the regulation of the Minister of Justice of 5th March 2004 on keeping court case files and transferring them to national archives or for utilisation, depending on the type of crime and the judgment issued, the case files are kept for another 3 to 50 years in court and then some categories of case files are transferred to national archives but others are destroyed.

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

Section 3: Admissibility of evidence before court

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

Answer: Indication of length of answer:

No. There are no separate rules or guidelines on the admissibility of electronic evidence. Admissibility rules are common for all types of evidence.

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

Answer: Indication of length of answer:

Yes. There no separate criteria for admissibility of evidence through mobile forensics. The rules of admissibility of evidence in context of data acquired from the mobile device has been widely discussed hereinabove in point 15.

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

Answer: Indication of length of answer:

Yes, as it has been discussed hereinabove in point 15, there is no automatic approach in excluding evidence acquired in breach of the law. The severity of procedural breach, its impact on credibility of evidence and on the fairness of proceedings and whether constitutional rights and freedoms were violated are the decisive factors for the court to decide whether the breach shall lead to complete inadmissibility of evidence.

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

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

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

I am not aware of any judicial rulings that would specifically address the issue. However, taking into account whole jurisprudence and the views of legal scholars on the admissibility of evidence in general, I am sure to express the view that such breach would not cause exclusion of the evidence since it does not harm in any way fairness of proceedings against the defendant.

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

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

I am not aware of any judicial rulings that would specifically address the issue. However, taking into account whole jurisprudence and the views of legal scholars on the admissibility of evidence in general, I am sure to express the view that such circumstance would not cause exclusion of the evidence since it does not harm in any way neither fairness of proceedings against the defendant, nor the credibility of evidence if all the methods used were correct and are properly documented.

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

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

No, there are no such rules. It is solely for the decision of the investigative bodies or the expert witness.

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

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

There are lots of judicial rulings on the issue of admissibility of evidence gathered under art. 19 of the Police Act with respect to the scope of the court's order. It has already been evaluated hereinabove in point 15. They basically deal with the issue of admissibility of evidence randomly gathered outside the scope of court's permission and at the moment the tendency to admit such evidence but only with respect to most serious crimes that would have justified the surveillance in the first place is predominant. However, some legal scholars present the view that any evidence gathered outside the court's permission (even by accident) shall be deemed inadmissible since it was only the court's permission that legalized infiltrating an individual's privacy[16]. These judgments do not address the methods of mobile forensics as such.

There is also one already cited judgment of 6th March 2017, II Kp 123/17, by the District Court in Zielona Góra. In the judgment the court granted the prosecutor's motion for procedural wire-tapping with regard to the search of a Gmail mailbox. The case is interesting because the prosecutor had already acquired the password to the account (the defendant had voluntarily given it) but nevertheless decided to apply for procedural wire-tapping, although so far the practice was rather that it would be treated under art. 236a C.C.P. That could suggest that the jurisprudence would tend to agree with the views of this part of the legal doctrine who claim that gaining access to the correspondence stored in the cloud always requires the decision on wire-tapping, not on the search under art. 236a C.C.P.

***46.* 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*

[16] D. Czerwińska, Problematyka zgody następczej na wykorzystanie tzw. przypadkowych znalezisk po 15.04.2016 r., Przegląd Sądowy 2019, no. 4, pp. 72-87.

followed for the evidence to be admissible? (as critical to the validity of evidence, their quality and impact evidence's acceptance by the courts)? If yes, please elaborate.

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

No. There are of course forensic standards but they do not affect the jurisprudence. Polish criminal procedure relies heavily on the rule of discretionary evaluation of evidence, set by art. 7 C.C.P. It is thus always for the court to assess the credibility of evidence. The court is only obliged to take into account the principles of logics and current knowledge, as well as general experience. It is underlined in the legal doctrine that it is neither possible nor desirable that the law or the jurisprudence would establish protocols or methods to be used by expert witnesses since it is their special knowledge that entitles them to choose best methods and protocols in the light of current knowledge[17].

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

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

Yes, it might be. Violating constitutional and conventional right to privacy and freedom of communication (art. 8 of the ECHR, art. 47 and art. 49 of the Polish Constitution) may lead the court to the conclusion that the evidence has been obtained illegally and is thus inadmissible. What is more, art. 51 of the Polish Constitution protects the personal data of any person and precises in section 4 that everyone is entitled to demand the correction and/or removal of the information which is untrue, incomplete or was obtained contrary to the law. It was argues in the legal doctrine that this provision is a sufficient and self-contained basis of excluding the evidence in criminal trial[18]. Compare the answer to question 15.

[17] See e.g. M. Skwarcow, M. Stępień, *Pojęcie, kryteria dopuszczalności i znaczenie dowodów naukowych w polskim i amerykańskim procesie karnym*, Przegląd Sądowy 2014, no. 9, pp. 102-113.
[18] J. Skorupka Jerzy, *Eliminowanie z procesu karnego dowodu zebranego w sposób sprzeczny z ustawą*, Państwo i Prawo 2011, no 3, pp. 80-85.

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

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

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

No, there is not. I have not found a single judgment specifically addressing the issue; there are no judgments cited in the papers dealing with this matter. Legal scholars tend to invoke American precedents to illustrate the issues but they have not yet been dealt with by Polish courts.

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

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

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

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

There are no general rules or guidelines. As it has been mentioned, Polish criminal procedure relies heavily on the rule of discretionary evaluation of evidence, set by art. 7 C.C.P. It is thus always for the court to assess the credibility of evidence. The court is only obliged to take into account the principles of logics and current knowledge, as well as general experience. Otherwise it is free to

assess all the evidence. There is also no closed catalogue of admissible evidence, so if new technologies of methods appear, there are no legal obstacles to use them.

Mobile forensic evidence is widely used in practice, especially in cases concerning serious and organized crime. It undoubtedly bears probative value.

There is no legal requirement that mobile device is examined by the expert witness but it is common practice. The other option that occurs in practice is that it is examined by the criminal analyst (usually tied to the Police). The result of such examination is a document called "criminal analysis", the evidentiary status of which is doubtful. It was argued in the legal doctrine that it might be treated as an expert witness if it in fact was produced as such (i.e. if the criminal analyst had previously been appointed by the prosecutor's or court's order as an expert in particular proceedings); otherwise, it is an official document[19]. The problem is that the document cannot substitute an expert witness's statement; in Polish criminal proceedings the issues that require special knowledge to be solved may only be adjudicated on the basis of an expert witness statements. Thus, the common practice is to appoint an expert witness.

It is underlined in the legal doctrine that it is neither possible nor desirable that the law or the jurisprudence would establish protocols or methods to be used by expert witnesses since it is their special knowledge that entitles them to choose best methods and protocols in the light of current knowledge[20].

There is no separate statute on expert witnesses in Poland. An expert witness may either be a sworn one, who is enlisted by the District Court or an *ad hoc* one, appointed by the investigating authority or the court for the purpose of particular criminal proceedings due to one's expert knowledge. In

[19] K. Woźniewski, *Charakter prawnodowodowy analizy kryminalnej*, Gdańskie Studia Prawnicze 2017, no. 2, s. 737-746.
[20] See e.g. M. Skwarcow, M. Stępień, *Pojęcie, kryteria dopuszczalności i znaczenie dowodów naukowych w polskim i amerykańskim procesie karnym*, Przegląd Sądowy 2014, no. 9, s. 102-113.

the latter case, assessing whether this knowledge is enough to provide sufficient quality belongs to the investigating authority or the court.

To become registered as an expert witness in the District Court, one shall fulfil the requirements set in the regulation of the Minister of Justice of 24th January 2005, especially in its § 12. Such person has to be at least 25 years old, enjoy full legal capacity, has special knowledge (there are no specific criteria) in a certain field, offer adequate guarantees of proper fulfilment of duties and consents to being enlisted.

As to the independence of the expert, art. 196 C.C.P. is the main procedural safeguard:

§ 1. Persons mentioned in Article 178 [defence attorney], 182 [relatives of the accused] and 185 [persons who have close relationships to the parties], as well as persons, who are disqualified for the reasons listed in Article 40 § 1 points 1-3 and 5 [acting previously in proceedings in another capacity] or summoned to act as a witness in a given case or who witnessed the offence, may not be called as experts.

§ 2. If the reasons for the disqualification of an expert mentioned in § 1 come to light, the opinion issued by him does not constitute evidence and - in place of the disqualified expert - a new expert is appointed.

§ 3. If information is revealed that undermines confidence in the expert's knowledge or impartiality, or other important information, a new expert is appointed.

The requirements for Police analysts are precisely regulated in regulation no. 3 of the Chief Constable of 17th January 2014 regarding competence to issue expert witness statements and conduct procedures in Police criminal laboratories.

There is no centralised management of mobile forensic operations.

50. **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.*

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

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

No, I am not.

51. **Question:** *Is there in your jurisdiction an established and recognised standardisation(s) of the processes of collection, analysis, interpretation and reporting of digital evidence that must be followed for the interpretation and presentation of evidence before a court? Or alternatively which is not obligatory but considered as critical for the validity of evidence, its quality or the impact of the evidence and its acceptance by the courts? If yes, please elaborate.*

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

No, there is not. As it has already been indicated, it is solely for the decision of the court whether it deems the evidence credible. The expert witness statement has to contain among others the report of actions carried out (art. 200 § 2 point 5 C.C.P.). In an expert witness statement all the methods used have to be explained in a way which makes it possible for the court to check correctness of the procedures conducted. If the court comes to the conclusion that the expert witness's statement is incomplete, unclear or if there are discrepancies in the statement or between different statements in the same proceedings, it shall call once again the same experts or appoint new ones.

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

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

There is no case law specifically addressing the issue.

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

Section 5: Implications of the use of mobiles forensics on the role of the different parties in the trial

53. **Question:** *Are there rules or guidance, or is there case law in your jurisdiction on how to respect the right to a fair trial in case of evidence extracted via mobile forensics? What practices are established in view of the respect of the principle of equality of arms?*

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

There are no rules, guidance or case law addressing the issue of fair trial in case of mobile forensics evidence. The equality of arms is understood as protected by the fact that the defendant has access to the evidence acquired (see point 60) and may challenge it, as well as the credibility of the expert witness's statement.

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

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

Mobile forensics is covered by the training programme for prosecutors (5 hours specifically for mobile forensics) and judges (10 hours for forensics in general) in the National School for Judges and Prosecutors. There are training courses available as well. Attending training courses is mandatory for all the lawyers but no provision obliges to attend courses on particular issue. The situation of expert witnesses has already been discussed – there is no particular training required by the law.

55. **Question:** *Is there a pre-determined time duration/limitation period required for the extraction of evidence from mobile devices, time for decoding, reviewing and analysing of the data, time for reporting that data in a form that prosecutors and others can use?*

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

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

There is no generally fixed term. The prosecutor or the court indicates a time limit when appointing the expert witness to examine a particular device. It is a huge problem in practice that mobile devices of suspects are seized and they are not returned for months, if not years.

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

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

The questions seems to broad to be properly answered.

In general Polish criminal trial is rather inquisitorial than adversarial.

The suspect/defendant enjoys all the rights provided for in art. 6 ECHR and more (right to defence, right to have three defence attorneys, freedom from self-incrimination, right to remain silent, right of access to the case file, right to file evidentiary motions right to give explanations, right to appeal). The defendant bears no criminal responsibility for false explanations. The main systemic problem with the position of the defendant in criminal proceedings is the overuse of pre-trial detention, frequently noticed by the ECtHR.

The victim is the party to the preparatory proceedings and may become a party at the stage of trial if he or she issues such statement before the opening statement of the prosecutor (art. 54 § 1 C.C.P.). He or she therefore enjoys all the rights of the party, especially right of access to the case file, right to file evidentiary motions and right to appeal. The victim has the right to oppose the resolution of the case in plea bargaining procedure and such opposition is binding to the court (art. 343, art. 387 C.C.P.). The victim also has the right to compensation and protection of privacy.

The prosecutor is the main investigative authority in preparatory proceedings. He may run them or order the Police to do so. He has broad competences and issues all the decisions apart from those that belong solely to the court (e.g. the decision on pre-trial detention). During trial the prosecutor is a party to the proceedings. However, new amendments tend to strengthen the position of the

prosecutor even in relation to the court (e.g. giving him the right to binding opposition against granting bail or concealing trial – art. 257 § 3 and art. 360 § 2 C.C.P.).

The court is an active participant of trial with the right to conduct *ex officio* evidence, which is very often used, even to the detriment of the defendant.

The witness is obliged to testify and tell the truth; he or she has the right to protection of privacy and return of costs.

5.1 The Prosecution

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

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

Mobile forensics and evidence are not mentioned in the regulation of the Minister of Justice of 7th April 2016 - Rules of the internal operation of common organizational units of the prosecutor's office. I am no aware of any requirements or guidance whatsoever. There might be some acts of internal nature, unavailable to the public.

5.2 The Court

***58.* Question:** *Is there judicial control over the approaches and methods used for acquiring, collecting and analyzing evidence? Please refer to case law if possible.*

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

Yes, there is. As it has been mentioned, the decision on seizure or search is subject to interlocutory appeal to the court which might declare it illegal (art. 236 § 1 C.C.P.). The decision on procedural wire-tapping is issued by the court and subject to the review of the court of higher instance under art. 240 C.C.P. The decision on operational control under art. 19 of the Police Act is issued by the District Court but is not subject to appellate review.

The review of acquiring, collecting and analysing evidence might also be done:

1) by refusing to grant the prosecutor's motion for conducting the evidence under art. 170 § 1 C.C.P.; in particular art. 170 § 1 point 1 obliges the court to dismiss the motion for conducting the evidence which is inadmissible,
2) even after admitting and conducting evidence the court is allowed and even obliged to disregard it if it seems inadmissible or incredible; there is no separate decision on the issue but it should be explained in the statement of reason for the judgment[21].

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

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

As it has previously been mentioned, Polish criminal procedure relies heavily on the rule of discretionary evaluation of evidence, set by art. 7 C.C.P. It is thus always for the court to assess the credibility of evidence. The court is only obliged to take into account the principles of logics and current knowledge, as well as general experience. Otherwise it is free to assess all the evidence and its assessment may only be successfully challenged in the appeal if the appellant proves that the assessment violated the rules of logic or knowledge or life experience. As it has previously been stated, I am not aware of judgments addressing specifically the issue of credibility of mobile forensics. From my own practice as a barrister I might add that such evidence is almost never challenged since all the participants to proceedings believe it to be very credible and unquestionable.

5.3 The defendant and defender

***60.* 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*

[21] J. Skorupka, *op. cit.*

the tools work, the procedures used, the parties involved and how the validity of the results is guaranteed)? Please refer to case law if possible.

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

The mobile evidence is part of the case file. The access of the defendant to the case file is regulated in art. 156 C.C.P. and it differs depending on the stage of proceedings. In preparatory proceedings the defendant generally has access to the case file, but the prosecutor may decline access if there is need of protecting the course of proceedings or important state interest. Such decision is subject to interlocutory appeal to the court. The prosecutor may not refuse the access to the evidence if it is the basis of a motion for pre-trial detention. The right of access to the case file involves acquiring copies of materials (also electronic ones). After referring the case to the court for trial, the access to the case file may not be declined to the defendant.

All the procedures used in acquiring mobile evidence – as it has already been mentioned – have to be precisely described in the expert witness's statement.

5.4 Witnesses

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

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

The privacy of the witnesses is preserved by art. 191 § 1a and 1b C.C.P. They provide that the witness's home address is established on the basis of his or her ID or written statement (since the oral statement could be heard by other participants of the interrogation, such as defense attorney) and that the questions asked cannot be directed at unveiling his or her domicile or workplace unless

these are important for the case. On the other hand art. 148a C.C.P. provides that the information on the witness's domicile, workplace, phone number and e-mail are not contained in the minutes of the interrogation but in a separate document which is stored in a separate file which is accessible only to the investigation authorities in the court. If such information are contained in certain documents in the case file other than the minutes, the copies of these documents, omitting these information, are put in the case file and the originals are transferred to the separate file hereinabove mentioned.

The only requirement to become a witness in criminal proceedings is the ability to observe and communicate observations.

5.5 The Victim

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

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

Victim is the party to the preparatory proceedings and may become a party at the stage of trial if he or she issues such statement before the opening statement of the prosecutor (art. 54 § 1 C.C.P.). The victim has the right to oppose the resolution of the case in plea bargaining procedure and such opposition is binding to the court (art. 343, art. 387 C.C.P.). Protection of the privacy of the victim is identical as in case of the witness (question 61). There are additional protective measures towards victims of sexual crimes and minor victims regulated in art. 185a-185c C.C.P., mostly constating in the rule of one-time-only interrogation and only by the court, with the presence of the psychologist and in some cases without the defendant having right to be present (only defence attorney does).

The victim's right to access the case file is the same as defendant (question 60), so of course the victim may use the evidence obtained via mobile forensics to exercise his or her rights.

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

Section 6: Comments

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

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