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.

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**

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

**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: Professor Inger Marie Sunde,** The Norwegian Police University College (NPUC) (Politihøgskolen), Research dept., Leader of the multidisciplinary research group "Policing in a Digitized Society".

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

**Answer:** Oslo, Norway.

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**:

***NOTE:*** *Unless otherwise indicated, all references to legal provisions relate to sections (§) in the Norwegian Criminal Procedure Act from 1981 (CPA):*[1]

The short answer is "No".

Longer answer: Mobile Devices (MDs) are covered by the terms

- "storage place" (Norw: "oppbevaringssted") in § 192 about search (Norw: "ransaking"),
- "object" (Norw: "ting") in § 203 about seizure (Norw: "beslag"),
- "computer system" (Norw: "datasystem") in
    - § 199 a about gaining access in order to search or examine a computer system,
    - § 216 o and § 216 p, about computer monitoring (Norw: "dataavlesing).

The provisions about search and seizure (§§ 192 and 203) have a long history stemming at least from the criminal procedure act from 1887 preceding CPA 1981. §§ 192 and 203 authorize search and seizure as traditional "open" investigation methods. In 1999 the CPA was supplemented with provisions authorizing "secret" search and seizure, i.e., search and seizure with suspended notification to the suspect / 3rd person targeted by the coercive measure. The provisions are § 200

[1] See Section 6.

a (secret search – "storage place") and § 208 a (secret seizure – "object"). Provisions included by law 3 December 1999 no. 82.

"Storage place" in § 192 / 200 a (search) originally covered physical storage places, such as a storage room, closet, chest or safe. By interpretation, the term now also includes computer systems, including MDs, and electronic storage media. The notion is that such systems, devices and media offer a place for storing electronic data.

"Object" in § 203 / 208 a (seizure) clearly encompasses all tangibles. However "object" is interpreted in a broad meaning also encompassing any other item which can be identified and specified, e.g. blood samples, biological traces, water in a bottle, electricity/KwH. Thus, also electronic information is an "object". It means that the copy secured by the police of data stored in a MD/a user account in the Cloud, is an object separately from the hardware on which it was stored. The legal effect is that the seizure of the MD may be lifted once the digital content is secured (and eventually seized, cf. Q17), and that the owner's right to challenge the seizure is activated individually with respect to the seized digital content, and the MD, respectively (Cf. Qs17 and 18).

The provisions using the term "computer system" are of more recent origin:

- In 2005: § 199 a; implementing the Cybercrime convention article 19.4 (included by law 1 July 2005 no. 16)
- In 2017: §§ 216 o and p; computer monitoring (included by law 17 June 2016 no. 54).

"Computer system" encompasses any item capable of automatic processing computer data (cf. the Cybercrime convention article 1(a) – def. "computer system"). Computer system falls under the scope of "object" in § 203. Both terms encompass fixed systems and MDs alike.

## Introductory comments relevant to understanding Norwegian criminal procedural law:

### Legal concepts:

*Search ("ransaking")* is a legal term referring to the police looking for objects that may be seized.

*Seizure ("beslag")* is a legal term referring to *a decision* to take an object out of someone's possession and into the possession of the police. The legal competence to make the decision is primarily held by the public prosecutor. The actual taking of the object is *an act* normally performed by the criminal investigator. This act does not have a procedural expression, but is often referred to as "securing" the object, and sometimes as "preliminary" seizure (Cf. Q17)

*Inquiry ("gransking")* is a legal term referring to the court's or an expert witness' examination of an object. The term is not used in relation to a criminal investigator's examination of an object, and the CPA does not say much about investigator's examination at all. In practice, the expressions "examining/examination" ("Norw: undersøke/undersøkelse") are commonly used.

Norwegian procedural law does not regulate the distinction between search and inquiry/examination in a detailed fashion. This causes some uncertainty i.a. with respect to MDs onto which electronic information is stored. The expert committee which drafted a proposal for a new Criminal Procedure Act (NOU 2016:24) pointed out that the stages between search, seizure and inquiry do not necessarily follow each other in that order (ch. 14.7.1, p. 332). (The expert group proposed a new legal provision about "examination of objects" – authorizing the police to examine objects in its possession, cf. draft § 18-7. "Examination" is then to be distinguished from "inquiry" signifying the court's/expert witness' examination of the object). In 2019 the Ministry of Justice commissioned a supplemental expert report specifically addressing digital search and seizure. The report is due 31 March, 2021. The other parts of the work of the expert committee has yet to be followed up by the MoJ.

## General conditions for the use of coercive measures:

**(i)** A certain degree of suspicion ("the suspicion condition"),
**(ii)** of the existence of a crime of a certain gravity ("the criminality condition"), and
**(iii)** that the coercive measure is necessary and not disproportionate ("the proportionality condition").

Items (i) and (ii) are described in relation to search and seizure further out in the questionnaire. Computer monitoring (§§ 216 o and p) generally follows conditions similar to secret search (§ 200 a). As computer monitoring possibly falls outside the scope of this questionnaire, it is not explained in detail.

As regards (iii) – the proportionality condition: The general conditions of necessity and proportionality are enshrined in § 170 a:

> "A coercive measure may be used only when there is sufficient reason to do so. The coercive measure may not be used when it would be a disproportionate intervention in view of the nature of the case and other circumstances."

The legal assessment pursuant § 170 a, closely resembles the legal standard "necessary in a democratic society" in ECHR article 8(2). The ECHR is implemented in Norwegian law, ranking between formal legislation and the Constitution (on top), cf. the Human Rights Act

("Menneskerettsloven") of 21 May no 30, §§ 2 and 3. The Constitution, Chapter E, *Human Rights*, contains guarantees, i.a. concerning fair trial (§ 95, cf. ECHR article 6), right to private life (§ 102, cf ECHR article 8(1)) and legality (§ 113, cf. ECHR article 8(2)). The provisions are relevant to this questionnaire. The Constitution § 92 states that Norwegian public authorities are obliged to *"respect and secure"* the human rights as enshrined, i.a., in the ECHR, thus expressing the State's negative and the positive obligation concerning those rights.

## 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

#### Introductory comment

"Mobile device not seized" may be understood in two ways: 1) That the police has not taken the MD into its possession; or 2) that the police has taken the MD in possession on a legal basis other than seizure, for instance consent. A valid consent must be informed and voluntary. The pressure experienced by a suspect confronted with the police, generally excludes consent, and the police must resort to seizure. More often consent may be relied on in relation to witnesses, including victims, but can be problematic in these situations as well. For instance a rape victim fearing that exposure of private videos on her smart phone - unrelated to the incident – may impair her credibility. By seizure pursuant to § 203, the police is forced to justify the taking of the MD, in relation to the legal conditions and safeguards. Also ownerless objects are included into a case by seizure, e.g. a smart phone found at an outdoor crime scene.

*The Qs below are answered under assumption 1, i.e. that the police does not have the MD in its possession.*

***4.*** **Under what circumstances can a mobile device be read or searched without seizing it?**

Reading or examining the content of a MD not in the possession of the police, must be performed remotely, like any search of a personal user account. The provisions about search (§§ 192/200 a) and computer monitoring (§§ 216 o and 216 p) are applicable.

An alternative is use of a production order requesting an Electronic Service Provider (ESP) to hand out information from or relating to the use of the user account (§ 210, 3rd para, see also Q28). ESPs have a duty of confidentiality, cf. the Electronic Communication Act (2003) § 2-9, an obligation which can be lifted by Nkom (the Norwegian Communications Authority) pursuant to CPA § 118. In practice, confidentiality is not lifted for stored content data, e.g. text-messages (SMS) or email. Requests concerning historic traffic and location data, and PUK-code, have a better chance of acceptance. This will be with notification to the end-user, for instance the suspect, cf. § 210, 4th para, or under slightly stricter conditions, without notification (i.e. postponement of notification for 8 weeks with a possibility for renewal) § 210 b. Yet an alternative, is seizure by the public prosecutor with notification (§ 203) or without notification (§ 208 a). Nkom's lifting of confidentiality (§ 118) is necessary in any case. *NOTE: The rules here are very patchy, as they have been tweaked over the years in efforts to keep up with the technological development, resulting in a set of rules which are difficult to fully comprehend and practice.*

Re: Future (real time) traffic and location data: In the investigation of offences with a statutory level of imprisonment of 5 years or more, ESPs may be ordered by the court to hand out traffic and location data *without notification* to the suspect (secret method) (§ 216 b). The order may only concern a MD registered to the suspect or a MD the suspect is deemed to make use of. The law does therefore not permit secretly collecting such data from a MD registered on a 3rd party *with whom the suspect is likely to communicate* (unless the suspect is deemed to actually make use of it, for instance a wife's or a flatmate's MD).

Provisions concerning *communication surveillance* (§ 216 a) are not applicable for collecting stored content data relating to a MD, as the scope is limited to concern communication *when in flow* between end-points.

### Remote search and computer monitoring:

*Search* is a one-off action not permitting the police to "linger" inside the user account over time. Although the CPA does not mention repeated search, the court (cf. Q 11) often grants a search period from date to date, and permits repeated search of the user account within this period. The practice has developed in relation to online search, and is not found in relation to physical search (of buildings, cars, etc.). In these cases the police may return solely in order to finalize a commenced search, for instance because it extends over a long time (e.g. search of a huge storage place), or the search was for some reason interrupted. The legality of said practice has not been an

issue before the Supreme Court, and it is well known, and reflected in the literature, e.g. NOU 2009: 15 (The Police Method Expert Committee – *Evaluation of police methods* – "Metodekontrollutvalget").

*Computer monitoring* differs from online search in that it lasts over time. It aims at collecting stored and/or volatile data (e.g. keystrokes). Computer monitoring was included in the CPA in 2017 primarily as a means to counter the encryption problem, which threatens to make both intercepted communication and stored data which has been secured, worthless to the police. By computer monitoring stored data may be read/copied while in the clear, and communication intercepted before/after en-/decryption, and encryption keys captured in real-time.

### Conditions:

Remote search of a user account:

**Open search:** May be performed *with* the knowledge of the owner (§ 192), either a suspect (§ 192, 1st para) or a witness (§ 192, 3rd para).

§ 192: "If any person is with just cause suspected of an act punishable pursuant to statute of imprisonment, a search may be made of his residence, premises or **storage place** in order to undertake an arrest or to look for **evidence** or **objects that may be seized.**

…

A search may be made on **any other person's premises** when there is just cause for suspecting such act, and

(1) …,
(2) …,
(3) There are special grounds to assume (…) that there may be found **evidence** or **objects that may be seized**"

General conditions regarding search - § 192

Search of the suspect's user account, § 192 1st para: (i) The suspicion condition: The required degree of suspicion is "just cause" (Norw: "skjellig grunn"), requiring a probability rate above 50%. The suspicion however, must be directed against the suspect, which means that solely a general suspicion that a crime has been committed – although with just cause - does not suffice. In such case the search must have basis is in 3rd para (see below).

(ii) The criminality condition: The crime must be of such gravity as to entail the possibility of imprisonment (as per the relevant criminal provision, i.e. "the statutory level" of punishment). It is

irrelevant that the punishment actually measured out by the courts, usually is much lower than the statutory level. In addition, as most criminal provisions include the possibility of imprisonment this threshold is not really much of a hindrance for search.

**NOTE:** *A "gut feeling" is never sufficient to underpin a certain degree of suspicion or other legal assessments. It is always necessary to point to some relevant concrete circumstances.*

Search of a 3rd party's user account, § 192, 3rd para, no. 3: Conditions (i) and (ii) are the same, except that the suspicion, naturally, is not directed at the 3rd party. The condition is that there are "special grounds" to believe that evidence/objects can be found on the user account. "Special grounds" must be based on concrete circumstances in the prevailing situation (cf. the NOTE above). For instance, that the 3rd party has the same social network as the suspect. "Special grounds" requires that it is more likely than not that evidence will be found at the search location (user account) (NLK-A1251)

With regard to search location: 3rd para does not mention "storage place", but the provision is interpreted to have the same meaning as 1st para, thus also including user accounts (NLK-A1245).[2] The interpretation was confirmed by the Supreme Court in a case from March 2019 (HR-2019-610-A, para 27).

**Secret search:** May be performed *without* the knowledge of the abovementioned persons – both suspects and 3rd parties (§ 200 a, 1st para). In relation to user accounts, secret search is probably more practical than open, as remote search is typically motivated by a need to keep the investigation secret from the suspect, or to act quickly before a user account is deleted.

(i) The suspicion condition: "Just cause" to suspect somebody…
(ii) The criminality condition: …of an act (including attempt), with a statutory level of imprisonment of 10 years or more, or of other criminal offences with lower levels of punishment, yet deemed to be of special gravity.
- Examples 10 years or more: Terrorism - the Norwegian Criminal Code (NCC) § 131, homicide - NCC § 275; rape under aggravating circumstances of a child under 14 years - NCC § 301.

[2] Here, the "unofficial" translation provided by the Ministry of Justice (see Legal Sources at the end of this document), is inaccurate in that it mentions the 3rd party's "premises", while the Norwegian authentic text says "hos andre", which literally means "by others". This expression is looser than "premises", and not necessarily associated with physical places.

- Examples other serious offences qualifying for secret online search: State espionage - NCC § 121, trafficking in human beings – NCC § 257, dealings with sexual abuse material of children – NCC § 311.

Remote computer monitoring:

Is a secret method performed *without* the knowledge of the owner of the user account (§ 216 o). Official translation of the provisions is not yet available. However, the material conditions are similar to those concerning secret search (cf § 200 a), only deviating on one point: As different from secret search, computer monitoring may only target computer systems or user accounts in the possession of the suspect, or which the suspect is deemed to make use of (§ 216 o, 4th para). The user account of a 3rd party thus only becomes a lawful target if the suspect is deemed to make use of it.

***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?**

§ 197, 3rd para: A search order shall

> "as far as possible be in writing and specify the nature of the search, the purpose of the search, and what it shall include".

From § 197 it follows that both the search order and the criminal charge define limits to the search. The search order specifies the *purpose* of the search and the *search location/object* (cf. "what it shall include"). In the context of a remote search of a user account the purpose is usually to look for and secure evidence that can be seized. The order should state this. Moreover, the order must identify the user account, e.g. by SIM/IMSI or IMEI number, or (if applicable) user name on an email or social media account.

Accounts not mentioned in the order cannot be searched. However, § 198, 1st para, no 3 contains an exemption, permitting a police officer to search an object on his/her own initiative. The conditions are:

> When there is **strong suspicion** of an act punishable pursuant to statute by imprisonment for a term **exceeding 6 months**, and there is an **imminent risk** that the search will otherwise be thwarted"

The provision gives legal basis for extending a search duly ordered (cf. Q11), for instance in the case of uncovering a secret hush mail account during the search. The police officer may search the hush mail account if there is an imminent risk that it cannot be accessed at a later stage, for instance due to deletion.

The criminal charge is the basis for specifying "the nature of the search", and forms the outer limit for what to search for. The search must look for evidence relevant to the criminal charge. This excludes the possibility of routine use of methods for instance to uncover child sexual exploitation and abuse material (CSEAM), when the charge concerns other forms of crime, e.g. economic crime, drugs, homicide etc. However, the scope of the criminal charge does not prevent the police from collecting evidence concerning other crimes, which they accidentally uncover. CSEAM material accidentally uncovered in a search relating to economic crime, may thus lead to extension of the criminal charge and prosecution.

Searching for evidence barred from seizure is not permitted, as it is regarded as arbitrary and against the rule of law. (Cf Q 19).

The proportionality condition (iii) is always a consideration (§ 170 a ).

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

Access to a user account in order to search it may be gained by use of *login data*, for instance discovered in other material collected in the investigation. This follows from § 200, 3rd paragraph which permits "break in" in order to perform a search of a building or a room, as applied *mutatis mutandi.*

It is not equally clear that the law also authorizes the use of *anti-forensics* (hacking methods) in order to gain access in a search (§ 192), especially if the police thus gains access to more resources than relevant, for instance at admin level instead of to the suspect's user account only. Yet, as this is a "break-in" as mentioned in § 200, the law literally does open for hacking in order to gain access. Rather, a limitation may be anchored in § 170 a (cited in Q3), on the view that such access may be considered unnecessary and disproportionate. The assessment is highly dependent on the prevailing circumstances, but the risk caused to other users of the service, in terms of exposure, disturbance or interruption of service, the sensitivity of the system, the number of users affected, the risk of causing problems to the service provider etc. are relevant elements. The issue has not as of yet, been tried before the courts.

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

Provided that the search order authorizes seizure, and § 204 is not invoked (cf. Q11), the information can be copied by the police. The police decides the method for securing the information

as per its own discretion, although within the limits of necessity and proportionality (§ 170 a and HR-2012-2035-U).

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

No, search is a coercive measure. However, a witness shall be present at the search "as far as possible", and sign the search report (§ 199). A police colleague may act as witness, for instance if the remote search is performed from the police quarters.

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

The question is not clear as the premise is that the MD is not in possession of the police. The answer is given in relation to Q21. § 199 a mentioned in Q21 applies also to user accounts.

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

In the case of an open search (§ 192), the owner of the user account must be informed in advance of the criminal charge and the search (§ 200, 1st para).

In the case of secret search (§ 200 a), the owner is informed at a later stage, as a main rule after 8 weeks, but the period may be extended (200 a, 4th para). However, the suspect has a right to be informed about the search *soonest possible* and not later than the point in time when s/he is criminally indicted, or the case is dismissed. (In some rare cases, the suspect has no right of information). The legal safeguard is that the court appoints a secret defense lawyer ("shadow" lawyer) (§ 100 a) acting on behalf of the suspect, with a right to be present in court meetings dealing with requests for secret search, control the legality of the search and the assessments relating to the conditions for the search. The secret defense lawyer is forbidden to get in contact with the suspect (§ 100 a, 3rd para).

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

The main rule is that search must be ordered by *the court*, cf. § 197 (open search) / 200 a, 1st para (secret search)

In case of urgency, *the public prosecutor* may order open search (197, 2nd para). The public prosecutor may also order secret search, if "delay entails a great risk that the investigation will be impaired" (§ 200 a, 6th para). In this case, the order is regarded as preliminary and must be controlled by a court within 24 hours.

Open search may also be decided by a police officer (criminal investigator) when there is "strong suspicion" of a crime which entails a statutory level of punishment of 6 months or more, and there is "imminent risk" that the purpose of the search will "otherwise be thwarted" (§ 198, 1st para, no. 3). See hush mail example provided in Q5. The provision is also applicable, i.a. when the police has seized a MD and wants to extend the search for evidence to user accounts accessible through apps on the device. (Cf. Q17).

The order must specify the account and be in writing. In case of time constraints, the order can be put into writing after the search.

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

User accounts of both a suspect and a 3rd party can be subject both to open and secret search. However, proportionality assessments may weigh in heavier in relation to 3rd party search than suspect search.

***13.* (and Qs 25 and 26):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.**

Norwegian law recognizes the principle of State sovereignty and the territorial limitation of enforcement jurisdiction (applicable to criminal investigation and use of coercive measures). § 4 explicitly states that the CPA applies "subject to such limitations as are recognized in international law or which derive from any agreement made with a foreign State".

The starting point therefore is that digital evidence located on servers abroad must be gathered through MLA. However, with respect to digital evidence accessible through digital networks, the approach is that Norwegian police may, under certain conditions, access the user account and download the content. The conditions are:

- That the conditions for search and seizure as per the provisions of the CPA must be fulfilled.
- That access is gained by *ordinary login procedure* with login data lawfully obtained by the police.
- That the account owner is on Norwegian territory, or at least is not known to have left the territory.

Under these circumstances the interference manifested on the territory of the foreign country is regarded as negligible (ordinary login, and copying) not constituting a violation of sovereignty.

Under circumstances when the whereabouts of the suspect/account owner is unknown, remote cross-border access may still be regarded as acceptable, at least, the opposite view has not yet been taken. This is under the assumption that the conditions for enforcement jurisdiction and adjudication are fulfilled. If the suspect is known to reside abroad, Norwegian authorities will try to transfer the case to that country.

The use of *anti-forensics (hacking)* in order to bypass ordinary login procedure, is a different case. Procedural law has not, as of yet, developed clear rules and safeguards relating to this method. If the method has notable effects on the ecom-service or its users (cf. Q6 for examples) it is likely to be regarded as interfering with sovereignty. Interestingly, § 216 p about computer monitoring (which i.a. includes targeting MDs and user accounts) explicitly authorizes hacking methods.

Only one case regarding these questions have been decided by the Supreme court so far, i.e. HR-2019-610-A (the Tidal case): The police searched a company's storage place for business operation data, in the Cloud. The server was located abroad and the country known. However, the police got login data from the company representative, and accessed the database in the presence of a defense lawyer and a witness from the company. Under the circumstances, the Supreme Court found that the conditions for search pursuant to the CPA were fulfilled, that no disturbance had been caused to the country where the server was located, and that he search did not violate sovereignty.

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

Secret search is permitted only in relation to crimes with a statutory level of punishment of imprisonment of 10 years or more, and some other serious offences with lower statutory level of punishment (cf Q4). Open search is permitted in most cases (Q4).

***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.**

Norwegian procedural law is dedicated to the aim of seeking *the material truth* of a case (i.e. to know "what actually happened"), to this end applying the principle of free production of evidence at trial (Norw: "fri bevisførsel"). The prosecution still has the burden of proof and guilt must be proved beyond any reasonable doubt. The material truth in combination with free production of evidence, forms the rationale underlying *the main rule* concerning admissibility, i.e., that a wrong

does not automatically lead to inadmissibility. On the contrary, the evidence may be produced at trial insofar as it is relevant and may shed light on the circumstances (is not superfluous). Evidence may only be barred if the wrong substantially interferes with fundamental rights.

On this background, the answer is: No, not following the applicable rules does not always lead to inadmissibility of evidence.

Claims of inadmissibility are determined on a case-by-case basis, and the outcome hinges a lot on concrete circumstances. The legal doctrine concerning inadmissibility is developed in case law and literature, and the CPA does not have provisions explicitly regulating this.

Some examples of wrongs that might lead to inadmissibility:

- A relative of the suspect is led to disclose login data to the suspect's user account. The police has neglected the duty to inform the relative of his/her right to silence (the right to silence when related to the suspect). The breach substantially contravenes the right to fair trial (the Constitution article 95 and ECHR article 6), probably resulting in inadmissibility.
- A secret search is performed without prior appointment and control by a secret defense lawyer. Same reasoning as above (fair trial).

Norwegian procedural law does not apply the doctrine "fruits of the poisonous tree". A wrong at one stage does therefore not have a domino effect detrimental to evidence gathered at a later stage.

Re: Wrongs impairing the quality of the evidence: The legal approach is that the court shall form its own opinion about the quality and trustworthiness of the evidence. The view is rooted in the procedural principle of *free assessment of the evidence.* Again, the rule is that evidence claimed to be impaired is still admissible, but the court proceedings will try to identify the wrong and get an explanation for it, control the quality of the forensic documentation in the case file, and get an understanding whether the wrong actually impaired the evidentiary value of the evidence or not. Procedural law emphasize *transparency* as a guarantee for *equality of arms.* A wrong which is not documented, may deprive the defendant of the possibility to adequately defend her/himself. In such case, fair trial is at stake, and the evidence may be inadmissible (or the case reopened).

## Mobile device seized

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

Yes, as an "object" it can be seized pursuant to § 203 (see also Q3):

> "Objects that are deemed to be significant as evidence may be seized until a legally enforceable judgment is passed. The same applies to objects that are deemed to be liable to confiscation or to a claim for surrender by an aggrieved person."

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

MDs are valuable sources of evidence and commonly seized in criminal investigations.

Conditions:
Re: (i) The suspicion condition: As for search (Q4) the required degree of suspicion is "just cause". Unlike § 192 (search) § 203 does not explicitly mention "just cause", but the interpretation is settled case-law since 2000 (HR-2000-290). It is not necessary that the suspicion concerns the person whose mobile device is seized (also this differs from § 192, 1st para).

Re: (ii): The criminality condition: § 203 does not set conditions with respect to the gravity of the crime.

Thus, (i) and (ii) may be expressed in one sentence, demanding that "it is more likely than not that a crime has been committed".

§ 203 also demands *relevance*, i.e., that the object must be "deemed" to be significant as evidence. A reasonable likelihood for such relevance is sufficient (NLK- N1406).

Procedure:
Primary legal competence to "decide" seizure is held by the public prosecutor (§ 205, 1st para). The decision is a legal disposition, i.a. activating the owner's right to challenge the legality of the seizure before a court (§ 208). From this point in time also § 213 is activated, stating the obligation of the prosecutor to lift the seizure in case there is "no longer any need for it".

The obligation to lift the seizure is relevant i.a., to MDs the seizure of which is motivated by the possible evidential value of the digital content only. Once the content is secured, the seizure of the MD should be lifted and the MD returned to the owner.[3]

Pursuant to § 206, 1st para, a police officer may "make" seizure (Norw: "ta beslag") when performing a search, and else "when delay causes a risk". From this position, § 198, 1st para, no 3, may give basis for proceeding further by searching user accounts accessible through applications on the MD. (cf. Q11). The firmer act of the police is regarded as *preliminary* seizure, to be reviewed

[3] There can be other reasons for still maintaining the seizure, e.g. securing subsequent confiscation.

by the public prosecutor who has competence to order that the seizure be "maintained" (§ 206, 2nd para). The right/obligation mentioned above is activated first at the decision of the prosecutor.

Objects seized must be specified in a "Report of seizure" (Norw: beslagsrapport) (§ 207). As an "object", electronic information copied from a MD, shall have a separate entry in the report linked to the MD from which it was secured (Cf. section 3.3 in Regulation by the Norwegian Police Directorate, regarding *Treatment of seizure in criminal investigation*, RPOD-2010-7, updated 19 June, 2017).

Some objects/information are legally protected from seizure (§ 204), see Q 19. Objections against seizure may be raised by the owner/suspect during a search, or it may be clear to the prosecutor/police already from the very beginning, that the seized material is likely to contain legally protected elements. The latter is typical when performing a search of a lawyer's office. In such case, the police may lawfully secure the material, then put it in a sealed box, and bring it to the court. The court filters through the material, removing the parts that are legally protected. The remaining material is handed out to the police for continued search. The files identified as having evidential value are picked out by the police and subsequently seized by the public prosecutor. From this point in time the right/obligation previously mentioned are activated.

The abovementioned procedure has been developed by the courts, based on analogous interpretation of § 205, 3rd. para:

> "Documents or anything else that the possessor is not obliged to testify about except by special order of the court may not be seized without a court order unless such a special order has already been made. If the police wish to submit documents to the court for a decision as to whether they may be seized, the said documents shall be sealed in a closed envelope in the presence of a representative of the possessor."

The legal privilege protecting lawyer's advice leads to strict protection by the court (an interpretation influenced, i.a. by the ECtHR judgments *Modarca v. Moldovia* [EMD-2005-14437] *Petri Sallinen and Others v Finland* [EMD-1999-50882]). There has been a string of cases concerning digital search in this regard, the latest: HR-2018-699-A. The cases deal with digital material in general, regardless of the kind of hardware from which it was secured. There are no cases where MDs were at issue as such.

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

As shown by the answer to Q17, the CPA from 1981 has not kept up with the technological development, and from 2010 the Supreme Court has decided on issues concerning digital search and seizure on a number of occasions. The Court has also expressed a need for improved regulation, and as mentioned (Q3), a report on the topic is due 31, March 2021.

Summarizing the main rules: We assume that the MD was lawfully *seized* (remembering that seizure is used both for MDs in possession of the owner, and for ownerless MDs (see end Q3)). The content of a seized MD can always be secured /copied. Examination of the content however, is regarded a *search*, thus the legal conditions for search as earlier described become activated. It follows that,

- In the case of a MD seized by a police officer pursuant to § 206, 1st para, (see Q11) without prior search order, the content cannot be examined until a warrant (search order) is obtained pursuant to § 197 (from either the court or the prosecutor).

- In the case of a MD seized during a duly authorized house search (§ 192 ff), and provided the search order authorizes seizure of MDs and subsequent search/examination of the content, the content can be examined. It is not necessary to obtain a new warrant/search order for this purpose. The content can be examined as many times as needed in light of the development of the investigation.

- Examination/search of the content is limited to the scope of the search order, which again is limited to concern the crime mentioned in the criminal charge. If the police wants to search the digital content for evidence relevant to other crimes, a new warrant from the court is necessary, as per § 197, and the conditions described in Q4 must be fulfilled. A consequence is that excess digital information secured from the MD may not be treated as "intelligence" shareable through the police' intelligence database. Instead, the digital copy must be kept in a storage place for investigation material. Issues regarding deletion and archiving of such material remains to be clearly regulated.

- Digital information regarded as having evidential value, shall be picked out and included in the case file. There it will disclosed to the suspect/defense lawyer, thus maintaining the right of contradiction.

- Digital information picked out from the secured content, is regarded as seized objects and shall be included in the report about seizure (§ 207). From this point in time, the suspect has a right to challenge the seizure before the court (§ 208). The act of securing the digital content for the purpose of conducting a subsequent examination/search, is regarded as intermediary and preliminary. The suspect does not have full procedural rights in this phase.

***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?**

§ 204 states that the police cannot seize

> "documents or anything else whose contents a witness may refuse to testify about pursuant to sections 117 to 121 and 124-125, and which are in the possession either of a person who can refuse to testify or of a person who has a legal interest in keeping them secret.
>
> The prohibition … does not apply to documents or anything else that contains confidences between persons who are suspected of being accomplices to the criminal act".

§ 204 protects objects (including digital content/information) such as a lawyer's advice, health information, journalistic sources, religious confessions and more.

As indicated in Q17 there is a presumption for legal protection when searching a lawyer's office and digital devices, and the procedure of court control must be followed (§ 205, 3rd para).

The police/prosecutor has a duty to remove privileged information they accidentally come across when searching content. Under such circumstances, court control is not required. This procedure applies equally to digital content secured by surveillance of communication.

MDs, typically smartphones, may be regarded as representing the core of the owner's private lifte, thus activating special concerns of necessity and proportionality. The issue has not become legally contested as of yet, but an interesting article on the topic was published last year, and is in the process of peer-reviewed re-publishing in *Nordisk Tidsskrift for Kriminalvidenskab (NTfK).* Full reference is: Nina Sunde, *Min mobil er min borg – smartmobilens rolle i privatlivet og i kommunikasjon [My cell phone is my castle – the role of the smartphone in private life and in communication].* Published in Vennebok til Ulf Stridbeck ved hans 70-årsdag, Boucht, J.-P. Høgberg, A-P (eds.), University in Oslo.

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

Not as regards the suspect, but in relation to a 3rd person (witness), yes.

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

Yes, pursuant to § 199 a 1st and 3rd paragraph, in conj. with 2nd paragraph:

> "When conducting a search of a computer system the police may order everyone who is dealing with the said system to provide information necessary for gaining access to the system or open it by use of biometric authentication.
>
> The police may force someone who refuses to comply with an order concerning biometric authentication as mentioned in 1st paragraph, to perform the authentication.
>
> A decision concerning the use of force pursuant to 2nd paragraph, shall be made by the public prosecutor. If delay entails a risk, the police present at the scene may make the decision. The decision shall immediately be reported to the public prosecutor.
>
> This provision applies *mutatis mutandi* to examination ("inquiry") of a computer system which has been seized pursuant to the provisions in chapter 18" *(i.e. §§ 203 ff., (author's comment)).*

The provision was originally included in order to comply with the Cyber Crime Convention article 19(4). In 2017 the scope was broadened also to include *biometric authentication*, and the use of force in this respect. The provision does not authorize use of force in order to make the suspect/3rd party *inform* the police about access data. But the police may *order* anyone "who is dealing with the said system" (the suspect and a 3rd party), to provide access.

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

Re: Open seizure (§ 203): The owner (possessor) of the MD shall be informed of the seizure and get a receipt (§ 207, 2nd para). The owner shall be informed of the criminal charge, the right to be assisted by a defense lawyer (§ 94) and of the right to challenge the seizure (§ 208).

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

As mentioned in Q18, examination of the content is regarded as a search, thus making the answer to Q6 relevant. The context of Q23 however, differs from the one in Q6 in that the MD/electronic content is in the possession of the police. The police therefore has better control with the method than when searching a user account in the Cloud (Q6). Because the search in the present context does not entail any risk to the ecom provider or its users, the freedom of the police to apply the methods is wider. In this case, then the answer is that the content secured from a MD may be examined in any way necessary for the investigation. This includes bypassing security measures, i.a., by use of login data or anti-forensic measures.

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

Not as per the law, but the proportionality assessment may be impacted.

***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.**
See Q13.

***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?**
Same as Q25.

***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?**

To my knowledge procedural law does not require a link between the MD and the user account in the Cloud. The MD and the user account are separate "storage places" in relation to § 192. The legal significance of a link between the MD and a user account in the Cloud, is that a police officer can extend a search from the MD to the user account, as per § 198, 1st para, no. 3 (see Q11), and secure the content of the user account asper § 206, 1st para (see Q17).

***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?**

Access data kept by and ESP (e.g. PUK), is confidential pursuant to the Electronic Communications Act § 2-9. The Nkom must lift the confidentiality (§ 118), whereupon the court can order the ESP to hand out the access data (§ 210) or the public prosecutor decides seizure (§ 203), which will have the same legal effect (see also Q4).

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

No, although the gravity of the crime does always weigh in heavily in a proportionality assessment.

***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.**

See Q15.

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

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

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

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

I have not been able to find this out. Generally, the Norwegian NCIS (Kriminalpolitisentralen/KRIPOS) is the central forensic expert organization in the police. To the extent that standards ans guidelines are developed, they should be distributed to local police, i.a. through the internal police system "Kilden" ("the Source").

*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?**

There are no *specific* rules in criminal procedure relating to the use of mobile forensic tools using/deploying AI-technology. Pursuant to the *general* obligation to ensure a sound basis for decisions (Norw: "forsvarlig avgjørelsesgrunnlag") regarding investigative steps and the issuance of a criminal charge or indictment, any risks relating to AI-tools must be disclosed and accounted for in reports included in the case file. The obligation is limited to actual risks relevant to the concrete case. It is not necessary to describe every theoretical risk associated with AI in general. The obligation to ensure a sound basis for decisions is enshrined in the principle of objectivity, laid

down in § 55, 4th para (prosecutor) and § 226, 3rd para (police). Further, § 294 expresses the obligation of the judge to ensure that the case is "fully clarified", which may result in request for new evidence and adjournment of the proceedings.

In the end, the likelihood of AI-related risks to become an issue is possibly to a high extent dependent on the respective actors' (including the defense lawyer's) ability to capture and describe them.

A recent Master Thesis (law) analyses the questions raised here. Written by Bendik Wollmann: *Utfordringer ved bruk av kunstig intelligens i behandlingen av bevis i straffesaker. En analyse av dagens bevissystem i straffeprosessen (Challenges with use of AI in relation to evidence in criminal cases. An analysis of the current evidence system in criminal procedural law]*. Tromsø University. June 2020.

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

A forensic examiner should act pursuant to a mandate made by the public prosecutor or the lead criminal investigator. With respect to a MD physically located abroad, the concern is how to secure it. In this case MLA is necessary. With respect to digital content on user accounts, the concern is primarily to ensure that the legal conditions as outlined in Q13 are fulfilled. This is not the responsibility of the forensic examiner, unless s/he is involved in the actual gathering of the digital material.

After the Tidal-decision (HR-2019-610-A) there is negligible risk that the digital evidence be inadmissible, provided that access was gained by ordinary login procedure. The risk of inadmissibility for evidence gained by hacking and account, is hard to assess. The method is lawful as per the CPA, so the question turns on the weight a possible violation of sovereignty is afforded, or on a principled approach to the question.

***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?**

Yes, this is a general procedure pertaining to all cross-border collection of evidence. Again, the fundamental requirement is that the conditions for collecting the evidence – if it had been located in Norway – are fulfilled.

***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?**

This depends whether Norway has a MLAT with the relevant country. See also I.M. Sunde *Cybercrime Law*, ch. 3.5. in A. Årnes (Ed.) Digital Forensics, Wiley, 2018.

***36.*** **Question: Are you aware of any existing cooperation mechanisms and practices with the private sector? Answer:** No.

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

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

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

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

As mentioned in Q18, the total amount of data, including excess information, cannot be shared indiscriminately via the intelligence databases in the police. The secured copy must be stored separately, and *the files identified as having evidential value* must be included in the case-file. To the extent that these files also have value as intelligence, they can be stored in the intelligence database (Indicia) as well, subject to the fundamental conditions concerning necessity etc (cf. the Police Register Act (PRA) § 5 ff). Intelligence must further be treated in conformity with the general rules of the PRA (transposing the Law Enforcement Directive 2016/680 EU into Norwegian law).

Other than the limits set by the criminal charge, the search order and the legal protection of privileged information, there are not any legal restrictions on the analysis of data from MDs. If the analysis accidentally uncovers privileged information, the police/prosecutor is obliged to remove and delete it.

Principles of evidence integrity and chain of custody underlie the procedural rules. As mentioned, there is an obligation to disclose any wrongs or alterations to the evidence. Evidence picked out from the secured data, is included in the case file and disclosed to the suspect/defense lawyer, and to the victim as the case may be.

Although the obligation to document each investigative step, including the analysis, is clear, the law is not detailed on this point. This might be regarded as a weakness of the law, and will perhaps be addressed in the expert report mentioned in Q3.

Privacy protection is enforced i.a. in relation to requests for disclosure of the total amount of secured data. The Supreme Court has taken the position that, equality of arms (fair trial) demands that the defendant has access to the same amount of information as the police (HR-2011-1744-A). The scope of the informational balance concerns information collected and analyzed by the police during the criminal investigation. The 2011-case concerned two defendants (A and B). B requested access to image copies secured from A's computers. The court rejected the request on the ground that it would interfere with the privacy and data protection rights of 3rd parties unrelated to the case. The police had used automated keyword search, and had not looked into material other than produced by the search. Furthermore, the police had provided B with access to the files produced by the search. As the police did not have an informational advantage over the defendant (B), Bs access to the information was correspondingly delimited. The Court emphasized the defendant's right to know the search criteria and suggest amendments to the analysis.

As regards *transparency* concerning the tools applied in the analysis, there has not been any clear case challenging this so far. However, the General Attorney (Norw: Riksadvokaten") expressed concern over the computer based tool "CrashCube" applied by the Norwegian Public Roads Administration (Norw: "Statens Vegvesen") in order to secure data from cars involved in accidents. It has turned out that there was errors both in the ways in which the data was secured, and how the data was interpreted. The General Attorney ordered a stop to all ongoing cases involving CrashCube (letter from the General Attorney to the Senior Prosecutors and Chiefs of Police, 20 December, 2019).

## 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?**

No.

***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.**

Yes. And see Q15.

***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?**

Yes, see Q15.

***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?**

As per the Tidal-case (HR-2019-610-A) search of a user account located abroad, without the permission of the other State, is not necessarily regarded as a violation of sovereignty. Hard cases may arise, but the outcome is difficult to estimate. Reciprocity is possibly a consideration. If Norwegian procedural law accepts evidence collected by unilateral hacking abroad, the method must be accepted also when performed against servers located in Norway.

***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.**

The matter of importance is that the alteration is disclosed. See previous answers on this. The alteration does not automatically lead to inadmissibility.

***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.**

No.

***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.**

No.

***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.**

No.

***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?**

In a case from 2014 concerning secret communication surveillance (§ 216 a ff), excess information was declared inadmissible on the ground that the police had neglected the statutory obligation to delete the information (HR-2014-2288-A). The purpose of the obligation to delete is to minimize the severity of the privacy interference caused by secret communication surveillance. The case signals increased awareness concerning the intrusiveness of technical investigation methods.

The law does not provide an obligation to delete digital evidence secured from stored data, e.g. from a MD, corresponding to the one pertaining to communication surveillance. However, the huge amounts of data (big data) secured almost by routine in criminal investigations, give rise to serious privacy concerns. Until more detailed regulation becomes available, stricter application of the proportionality assessment may prove to be an option.

***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.**

Not to my knowledge.

## 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?**

No. Expert witness is an option, but not mandatory.

These issues have attracted increased attention as of lately, e.g.:

- Nina Sunde *Digitale bevis – menneskelige feil [Digital evidence - Human Errors]*, in: Det digitale er et hurtigtog – Vitenskapelige perspektiver på politiarbeid, digitalisering og teknologi [The digital is a high-speed train – Scientific perspectives on police work, digitization and technology], Fagbokforlaget, 2019. (Book chapter)
- Tom Erlandsen *Fallacies when Evaluating Digital Evidence Among Prosecutors in the Norwegian Police Service*, NTNU (masters thesis – Information Security), 2019.

  https://ntnuopen.ntnu.no/ntnu-xmlui/handle/11250/2617771

***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.**

No.

***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.**

No, the main reason being the principle of free production of evidence (Q15). There is an increasing pressure however, for guidelines and expertise in this respect. The issue concerns all digital evidence, not MD evidence in particular.

Nina Sunde, PhD-researcher and police superintendent with the NPUC, is an expert in the field, and may be contacted on: ninsun@phs.no.

***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.**

No. Un/reliability is not a valid ground for inadmissibility (Q13)

## 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?**

I think this has already been answered. I do not have anything to add.

***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?**

No, and this is an increasingly hot topic.

***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?**

No. But the time-consuming forensic procedures and the vast amounts of data is a serious concern in relation to trial within "reasonable time" (ECHR article 6, the Constitution § 95 – fair trial).

***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.)?**

### The Prosecution:

The prosecution has the burden of proof and must prove guilt beyond any reasonable doubt. The prosecution is the formal/legal leader of the criminal investigation (§ 225), and responsible for the use of coercive measures, such as search and seizure. The prosecution is further responsible for ensuring the legal rights and safeguards of the suspect/defendant, such as:

- Informing the suspect of the criminal charge and of coercive measures applied against him/her
- Initiate the appointment of a defense lawyer
- Ensuring the completeness of the case file
- Providing access to the case file/evidence
- Perform addition investigative steps if requested by the suspect
- Involve the suspect / defense lawyer in the criteria for automatic search of digital evidence

- Inform the defendant / defense lawyer about the criminal indictment and the evidence brought against the defendant
- The prosecutor is under a duty of objectivity. If the evidence does not bear, the prosecutor is obliged to drop the case, or if at trial, request acquittal.

## The Court

- Controls the legality of search, including the protection of privileged information
- Is not involved in the collection of evidence during the investigation
- Appoints a defense lawyer when the suspect becomes criminally charged
- Presides over the court proceedings and has an obligation to ensure that the case is "fully clarified" (§ 294). If not, the proceedings may be suspended or end with acquittal (reasonable doubt).
- Has very little power to declare evidence inadmissible.

## The defendant

- Has a right to be informed of the criminal charge and of coercive measures against him/her
- Right to access the case documents including the evidence
- Right to suggest supplemental investigative steps, e.g. additional analysis of digital evidence
- Right to challenge seizure
- Right to have seizure lifted when no linger necessary for the case
- Right to a defense lawyer
- Right to access to the secured data in total if the police has looked into it all. If the police has only looked into "matches" from an automated search, the defendant's access may be correspondingly limited.

## The witness/victim

- A right to be present at trial after s/he has given his/her own witness statement
- A witness with status as victim or relative to a deceased victim, has a right to access to the case file and evidence
- Victims of (sexual) assault, violence, human trafficking etc, is entitled to a "supporting" lawyer (Norw: Bistandsadvokat), as support in the investigation, the preparation of the case and at trial. A supporting lawyer is appointed at the cost of the State.

## 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?**

No.

## 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.**

Only as already described, i.e. court control with coercive measures and protection of privileged information, and the court's obligation to ensure that the case is "fully clarified" (§ 294).

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

There is free assessment of evidence. However, the court will control evidence integrity and chain of custody. Expert witness may also be heard.

## 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.**

This is not explicitly regulated. However, case law concerning huge data amounts has declared a right of the defendant to have an influence on search criteria, and at least to know the criteria and the tool used in a search.

## 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.**

Not sure I understand the question, but I give it a try. During the pre-trial stage, search (and analysis) is limited by the criminal charge. Effective safeguards controlling that the investigator does not look into irrelevant and private information are lacking.

Irrelevant information should not be made accessible to others, and the police is under a duty of confidentiality in this regard (the PRA §§ 23 ff).

## 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.**

Same as above.

## 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.**

The questionnaire is interesting enough, but it has been hard to see how MDs are any different from other computer systems also relevant to criminal investigations. My answers relate to statutory law and case law not specifically dealing with MDs (or evidence was secured from a MD, but this was not a significant fact in itself). Having contributed to the project, I hope I get to know the outcome of the research.

Best wishes

Inger Marie Sunde

### Online service for legal sources

Norwegian legal sources (acts, regulations, guidelines, case-law and much more) are available on the online service Lovdata: https://lovdata.no/

### Statutes

Unless otherwise indicated, all legal provisions (§ = section) refer to

- the Norwegian Criminal Procedure Act ("Straffeprosessloven") (CPA) of 22 May 1981 no. 5. Unofficial translation to English provided by the Ministry of Justice: https://app.uio.no/ub/ujur/oversatte-lover/data/lov-19810522-025-eng.pdf

Other statutes herein mentioned:

- The Norwegian Constitution ("Norges Grunnlov") of 17 May, 2014.
- the Electronic Communication Act ("Ekomloven") of 4 July, 2003 no 83
- the Human Rights Act ("Menneskerettsloven") of 21 May no 30
- the Police Register Act ("Politiregisterloven") (PRA) of 28 May, 2010, no. 16, (as amended 21 June 2019 no. 50).

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

## Legal doctrine (jurisprudence)

Annotations to the CPA: *Norsk Lovkommentar* ("NLK"), by Sunde Haugland, Geir, Rettsdata, Gyldendal, Oslo, Updated per 9 February 2020. https://www.rettsdata.no/ (not available in Lovdata)

- Referenced as NLK-A (A = Annotation) + number, e.g. NLK-A1405.