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: This questionnaire was completed by Charlotte Conings and Hans Van Bavel, respectively associate and partner of the criminal law team of the Stibbe law office in Brussels.

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

Answer: In Brussels, Belgium.

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

Answer: No legal definition exists of the notion 'mobile device' under Belgian law, at least not to our knowledge. Criminal law only refers to 'information systems' or 'computer systems' (hereinafter, we will consistently use the notion 'computer system'). The notion 'computer system' is defined very broadly in the preparatory works of the law of 28 November 2008 on computer related crimes: "*A system for the storage, processing or transfer of data. This includes in particular computers, chip cards and so on, but also networks and parts thereof, as well as telecommunication systems or parts thereof which make use of IT*". The notion thus covers a broad category of devices and systems, such as computers, laptops, smartphones, tablets, smartwatches, digital cameras, MP3-players, navigation devices, drones, but also apps, wireless networks, wifi-hotspots, etc. It thus refers, among others, to 'mobile devices' as covered by this project.

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?*
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?*
6. *Is it allowed to use technical tools to bypass security?*
7. *Can information be copied or only read at this stage?*
8. *Is consent of the owner/person in possession of the mobile device necessary?*
9. *Can the owner/person in possession of the mobile device be forced to unlock the device?*
10. *Must the owner/person in possession of the mobile device be informed?*
11. *Who can order a search and what are the formal requirements, if any?*
12. *Does it matter whether this person is the accused or witness/third party or the victim?*
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.*
14. *Does any of the foregoing depend on the type of crime involved (e.g. terrorism, child pornography etc.)?*

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.*

Mobile device seized

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

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

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

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?*

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

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

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

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

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

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

26. *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?*

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?*

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?*

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

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

Please, 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.

1. General legal framework of Belgian criminal investigations

In order to have a clear understanding of the possibility to search mobile devices during a Belgian criminal investigation, it is important to have a clear view on a few basic principles relating to Belgian criminal investigations:

The Belgian investigative stage of criminal proceedings is mainly inquisitorial. Two types of pre-trial investigations can be distinguished: the preliminary inquiry and the judicial inquiry. A **preliminary inquiry** is led by the **public prosecutor**, while a **judicial inquiry** is led by an

(impartial and independent) **investigating judge**. Such inquiry is required as soon as an investigative measure which belongs to the sole competence of the investigating judge has to be applied. Measures belonging to the sole competence of the investigating judge are typically measures which are considered very privacy-intrusive and far-reaching (e.g. home searches, wiretaps, covert computer searches, …). The investigating judge is furthermore competent to apply the measures which belong to the competence of the public prosecutor.

Since the procedural regime in case of a judicial inquiry is burdensome (including amongst others a mandatory judicial supervision), the legislator introduced a simplified procedure called "**mini judicial inquiry**" (art. 28*septies* CCP). In this procedure the intervention of the investigating judge is limited to a one-off authorisation. As a result, certain investigative measures which belong to the sole competence of the investigating judge, no longer require the start of a judicial inquiry and the investigation remains in the hands of the public prosecutor. However, the investigating judge retains the option of taking over the investigation, which entails the start of a full blown judicial inquiry, despite the limited request of the public prosecutor for a mini judicial inquiry. Specific investigative measures are furthermore excluded from the mini judicial inquiry and thus always require the start of a judicial inquiry.

In general, criminal investigations can only take place further to **serious and specific indications** that an offence has been or will be committed. The presence of such indications is therefor in principle a prerequisite for the application of all kinds of criminal investigative measures. However, in specific circumstances, **reasonable presumptions** that offences have been committed or will be committed, suffice and allow the start of a **proactive criminal investigation** (art. 28*bis* §2 CCP). The proactive investigation is however limited to offences which are or will be committed in the framework of a criminal organisation or which are included in the list of serious offences of Article 90*ter*, §§ 2-4 CCP. A proactive investigation can furthermore only be initiated upon the written approval of the public prosecutor, while a reactive investigation presupposes an immediate notification to the public prosecutor. Measures belonging to the sole competence of the

investigating judge can furthermore never be applied in the framework of a proactive investigation. These measures thus always require serious and specific indications of guilt.

To be more concrete:

- If in our answer to your questions, we mention that an investigative measure belongs to the competence of the police or public prosecutor, this measure can be applied as soon as:
    - Serious and specific indications of an offence exist or
    - Reasonable presumptions exist of an offence committed in the framework of a criminal organisation or included in the list of serious offences of Article 90*ter*, §§ 2-4 CCP;
- If in our answer to your questions, we mention that an investigative measure belongs to the competence of the investigating judge, this measure can be applied only if:
    - Serious and specific indications of an offence exist.

Depending on the concrete investigative measure, additional requirements will have to be met, as mentioned in our answer further down below.

2. General structure of the law governing criminal computer searches

As far as the search of computer systems in the framework of a criminal investigation is concerned, Belgian law makes a distinction between investigations of private computer systems and investigations of publicly accessible computer systems or data (such as open source data). Since we understand that the focus of this project is mobile forensics of private mobile systems (of a suspect, witness, victim, etc.), we will limit our advice to investigations of private computer systems.

As far as private computer systems are concerned, the Belgian Code of Criminal Procedure (hereinafter CCP) makes a clear distinction between

(1) transparent/open/non-covert investigations of computer systems (art. 39*bis* CCP and 88*ter* CCP)

(2) covert investigations of computer systems (art. 89*ter* CCP and 90*ter*-90*decies CCP*).

As far as the first category is concerned (i.e. transparent investigations), a further distinction is made between (a) investigations of computer systems which are not seized but can be subject to seizure, (b) investigations of computer systems which are seized, (c) remote investigations of computer systems (network search) and (d) all other transparent investigations of computer systems.

For the second category (i.e. covert investigations) a distinction is made between (a) an orienting and limited sneak and peek and (2) a covert computer and network search.

In answering your questions, we will start from the main distinction as provided by you, i.e. searches of mobile devices not seized and searches of mobile devices which are seized and fit the abovementioned Belgian legal regime of computer searches into this main distinction.

3. Application to the case of searching mobile devices

a. Mobile devices not seized

i. Transparent investigation

Relevant scenarios

A suspect, a witness or a victim 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, …

Transparent Computer Search

General principle: The **public prosecutor** has the power to order a search of a computer system that can be, but is not seized (art. 39*bis* §2 CCP). A consent of the owner/person in possession of the mobile device is not necessary.

As to the competent authority, an important nuance has to be made however. If the mobile device is located in a **private premise** and law enforcement agencies have to enter to premise in order to get access to the device, a home search will have to be applied. In principle, a home search can only be performed or ordered by an **investigating judge** in the framework of a judicial investigation. The order of the investigating judge should be in writing, reasoned and should indicate the scope and object of the search (which in practice is often drafted in rather broad terms). The search of mobile devices which are not seized will, in our view, only be allowed in as far as it clearly appears from the home search order or an separate order that such search was indeed ordered by the investigating judge leading the investigation. The home search is not limited to a certain list of offences or linked to a penalty threshold. The general principle of proportionality applies (cf. Art. 8 ECHR; *infra*). Specific rules apply to protect professional secrecy. With regard to the home search, exceptions exist however to the sole competence of the investigating judge, more specifically in case of consent of the resident or when the suspect is caught in the act. In those circumstances, a home search can also be applied in the framework of a preliminary inquiry led by the public prosecutor.

In principle, the public prosecutor (/investigating judge) can order the search of a computer system as soon as he has reasons to believe that the system contains data relevant for the investigation of the criminal offence he is investigating. This could be a computer system of an accused, just as well as a computer system of a witness, victim or third party. There is **no explicit limitation** as to which types of data can be searched nor as to the type of offence under investigation. The computer search is however limited to the data stored on the system. The public prosecutor can furthermore limit the scope of the search in his order but the law does not contain any specific rules in relation to such limitation of the scope of the search. As a general rule, and further to art. 8 ECHR and data protection laws (*infra* question 37), investigative measures should always be applied in a **proportionate** manner.

The law does not specify explicitly whether the order should be **in writing**, however, given the written nature of the criminal investigation, it seems recommended to provide a written order to avoid discussion in court.

Special rules apply if the mobile device belongs to **lawyers or a doctor** in order to protect professional privilege. The computer system of a lawyer or doctor may only be searched if they themselves are suspected of having committed or participated in the commission of a criminal offence or if precise facts give rise to suspicion that third parties suspected of having committed a criminal offence are using their electronic communication means. Furthermore, the President of the Bar or the representative of the Provincial Medical Association have to be informed of the measure. Information deemed to be covered by professional secrecy will not be included in the official report of the execution of the measure. Moreover, as a general rule, data relating to **journalistic sources** may not be the subject of an investigative measure, nor, therefore, of a computer search.

The law allows the use of technical tools to **bypass security**. In the framework of a transparent computer search, the competence to bypass security measures, if needed by technical means, or to apply technical measures to decrypt data which are stored on the computer system belongs to the public prosecutor (Art. 39*bis*, § 5 CCP). Furthermore, the owner/person in possession of the mobile device may be forced to unlock his device upon the order of an investigation judge further to art. 88quater CCP.[1]

If data are deemed to be useful for finding the truth, restitution, forfeiture, protection of civil interests or to stop the commission of a criminal offence and the seizure of the computer system is

[1] Cass. 4 February 2020, AR P.19.1086.N; GwH 20 February 2020, nr. 28/2020; C. CONINGS, R. DE KEERSMAEKER, "To save but not too safe: hoogste Belgische rechters zien geen graten in het decryptiebevel voor de verdachte", *T. Strafr.* 2020, afl. 3, 163-175; C. CONINGS, J. KERKHOFS, "U hebt het recht te zwijgen. Uw login kan en zal tegen u worden gebruikt? Over ontsleutelplicht, zwijgrecht en nemo tenetur", *NC* 2018, afl. 5, 457-472; J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime 3.0*, Brussel, Politeia, 2019, 561-566; C. VAN DE HEYNING, "Het zwijgrecht in digitale tijden: de strijd om decryptiesleutels naar het Grondwettelijk Hof", *T. Straf.* 2019, afl. 6, 307 e.v.

not desirable, those data and data necessary for understanding them, **may be copied**[2]. Also, data which are deemed to include relevant data may be seized in as far as this is deemed necessary to allow investigating the data (because of the practical impossibility to investigate the data on-site[3]. In other words, the investigators could opt for seizing the data on a computer system in order to allow them to investigate those data instead of materially seizing the computer system in order to allow them to investigate the system.

Article 39*bis*, § 7 CCP stipulates that the public prosecutor (or investigating judge) has to **notify** the person in charge of the computer system of the computer search and provide him with a summary of the data that are copied, made inaccessible or removed. This duty applies as far as the identity or residence of the said person can reasonably be established. The Constitutional Court has clarified that "the person in charge of the computer system" refers to the person or persons responsible for the data or communication stored on the computer system in question. This includes the suspect who does not have effective control over the computer system in question, but whose data are the subject of the search[4].

Transparant remote search

As mentioned above, the computer search only allows accessing data stored on the computer system under investigation. Belgian law also provides several possibilities to investigate information which is **stored on remote servers** (such as in the Cloud).

Art. 88*ter* CCP specifies the network search. This provision stipulates that the abovementioned computer search may be extended to linked computer systems, which are situated somewhere else. The network search may not go beyond the computer systems to which the persons entitled to use

[2] Art. 39*bis* §6 CCP; Cass. 22 October 2013, AR P.13.0550.N.; C. CONINGS, S. ROYER, "Verzamelen en vastleggen van digitaal bewijs in strafzaken" *NC* 2017, 330.
[3] C. CONINGS, *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Antwerpen, Intersentia, 2017, 324-325; C. CONINGS, S. ROYER, "Verzamelen en vastleggen van digitaal bewijs in strafzaken" *NC* 2017, 329. Cf. concerning physical evidence: Cass. 20 November 2001, AR P.000548.N, *Arr. Cass.* 2001, 1968.
[4] GwH 6 december 2018, nr. 174/2018.

the computer system under investigation, have access. Art. 39bis §4 CCP furthermore provides for the possibility to perform any other kind of transparent computer search not covered by the search of a seized (*infra*) or 'seizeable' computer search (*supra*). This article allows for instance the search of remotely stored data directly from the computers of law enforcement and allows accessing data even if there is no app on a mobile device of a suspect or other involved party that links to the data searched for or any other direct link from a mobile device. Since such a search always entails an extension of an investigative measure to data stored elsewhere, art. 39bis §4 CCP should be read together with art. 88*ter* CCP relating to the network search[5].

The **investigating judge** is the competent authority to order remote searches. The measure may be ordered in as far as it is necessary to reveal the truth about the criminal offence under investigation and in as far as other measures would be disproportionate or if there is a risk that evidence would be lost without this extension.

In the event of extreme urgency, the investigating judge may **orally** order the remote search. The order shall be **confirmed in writing** as soon as possible, stating the reasons of extreme urgency.

The competence to **bypass security measures** or to apply technical measures to decrypt data also belongs to the investigating judge (Art. 39*bis*, § 5 CCP).

If it turns out that the data, found through the extension of the search, are **not situated on Belgian territory**, they can still be copied according to Belgian law. In that event the authorities of the state concerned will be notified, if this state can be reasonably identified. According to Belgian law, the data can thus be accessed directly, even if the location of the server or identity of the service provider cannot be established.

The rules on seizure of data and notification are the same as described above in relation to transparent computer searches (*supra*).

[5] J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime 3.0*, Brussel, Politeia, 2019, 254.

ii. Covert Investigation

Relevant scenarios

Mobile devices may be found during a covert sneak and peek operation or during another secret investigative measure, law enforcement authorities may be aware of a way to remotely and secretly access a mobile device of a suspect, witness, third party, …

An IT sneak and peek or covert computer search can be applied, depending on the aim of the investigative measure (rather investigation-orienting or a full-blown search/real time monitoring of the computer system).

IT sneak and peek

Art. 89*ter juncto* 46*quinquies* CCP provide for the IT sneak and peek, which refers to a covert access to and a search of computer systems with a view to **orienting** the criminal investigation. Article 89*ter* CCP more specifically provides for the possibility to access a computer system at any time **without the knowledge or consent** of the owner or authorized user, for one of the purposes provided by law.

A IT sneak and peek operation can indeed only be used for limited purposes. The operation can only take place in order to

(i) carry out reconnaissance of the computer environment and verify the presence of data that are the object of the offence, that served or were meant to serve for the commission of the offence or that proceed from the offence;

(ii) gather evidence of the presence of these mentioned goods.

The goal of the sneak and peek operation cannot be the seizure of evidence, but can only be the establishment of the presence of evidence, for example by taking pictures or samples. If certain data require further investigation, some of them **could be copied by way of sampling**, meaning a limited amount of data may be copied with a view to further investigate those data. The preparatory

works give the example of coping a few images to investigate whether they indeed constitute child pornography.[6]

The possible **object** of the IT sneak and peek is **limited**. An IT sneak and peek operation can only take place vis-à-vis computer systems for which a suspicion exists that the mentioned data can be found there, that evidence of the presence of those data can be gathered or that they are being used by persons under suspicion. There is **no limitation** as to what **types of data** can be searched.

Since the notion 'computer systems' is defined broadly (*supra*) and the law does not provide for a limitation to the data stored on a physical computer system under investigation, the IT sneak and peek can also be performed vis à vis a **Cloud**-environment in as far as ordered by the competent authority. The measure therefore also allows accessing data even if there is no app on a mobile device of a suspect or other involved party that links to the data searched for or any other direct link from a mobile device. In contrast to art. 88*ter* CCP (*supra*) and art. 90*ter* CCP ff. (*infra*) art. 89*ter* CCP does not provide for a specific regime if the data happen to be located on servers abroad.

The **investigating judge** has the power to order this investigative measure. The measure is excluded from the mini judicial inquiry and thus requires a full-blown judicial inquiry.

The principle of proportionality demands that serious indications are present that the behaviour constitutes or would constitute an offence mentioned in a list of **serious offences** (list of Article 90*ter*, §§2-4 CCP) or an offence committed within the framework of a **criminal organisation**. The principle of **subsidiarity** demands that less intrusive means of investigation appear insufficient to reveal the truth.

A **written substantiated order** is necessary. In case of emergency, an oral decision suffices, but needs to be confirmed in writing as soon as possible.[7] When ordering the measure, the competent

[6] MvT, *Parl. St.* Kamer 2015-16, nr. 54K1966/001, 51.
[7] Art. 46*quinquies*, § 1 CCP.

authority must ensure respect for the proportionality principle, making sure the measure is limited to what is necessary in the light of establishing the truth.

In contrast to art. 39*bis* CCP (*supra*) art. 90*ter* ff. CCP (*infra*), art. 89*ter* CCP does not provide for an explicit possibility to **bypass security measures**. The IT sneak and peek is however a coercive measure, entailing in principle the possibility to overcome every obstacle to performing the measure. It is therefore accepted in doctrine that the measure includes the possibility to bypass security measures.[8] The question relating to the possibility to force the owner/user to unlock the device is not relevant in the context of a sneak and peek since the owner/user will be unaware of the investigative measure.

The law does not stipulate that the owner/user should be informed at a certain moment in time about the investigative measure.

Covert computer & network search

Art. 90*ter* CCP ff. provides for the possibility to perform a covert computer search, i.e. to break into computer systems in order to search for private data or to monitor the use of private data in real time. Art. 90*ter* CCP more specifically refers to the power to intercept, access, search and register not publicly accessible data in an IT-system or a part of it by technical means. The measure is applied covertly, i.e. without the knowledge and consent of the owner/user of the computer system. The measure implies the possibility to copy data.

Since the notion 'computer systems' is defined broadly (*supra*) and the law does not provide for a limitation to the data stored on a physical computer system under investigation, the covert computer search can also be performed vis à vis a **Cloud**-environment in as far as ordered by the competent authority. Art. 90*ter* CCP furthermore explicitly provides for the possibility to 'extend' the search to linked computer systems. Given the broad definition of 'computer system', the measure, in our view, also allows accessing data even if there is no app on a mobile device of a suspect or regular

[8] C. CONINGS, *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Antwerpen, Intersentia, 2017, 239; J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime 3.0*, Brussel, Politeia, 2019, 431-432.

contact of the suspect that links to the data searched for or any other direct link from a mobile device. If it turns out that the data, found through the measure provided by art. 90*ter* CCP, are not situated on Belgian territory, they can still be copied according to Belgian law. In that event the authorities of the state concerned will be notified, if this state can be reasonably identified (art. 90*quater* §5 CCP). According to Belgian law, the data can thus be accessed directly, even if the location of the server or identity of the service provider cannot be established.

The **investigating judge** is the sole competent authority, except for some limited competence[9] for the public prosecutor in case of a *flagrant délit*. The public prosecutor is in charge as long as the situation of flagrant délit continues, and with regard to the terrorism offences, during at least 72 hours after the flagrant délit has been discovered. The measure is excluded from the mini judicial inquiry and thus requires a full-blown judicial inquiry.

In view of this investigative measure, the investigating judge can also order the secret entry of a private site or residence, the **bypassing of security measures** of a computer system or the decryption of data by technical means. The question relating to the possibility to force the owner/user to unlock the device is not relevant in the context of the covert computer search since the owner/user will be unaware of the investigative measure.

Article 90*ter* CCP mentions the requirements of necessity to uncovering the truth and subsidiarity, implying that no less intrusive investigative measure is more appropriate. Article 90*ter* CCP **limits the scope** of the covert access to private communications and private data in a computer system furthermore in two ways:

(i) the investigative measure can only be directed at persons who, on the basis of serious indications, are suspected of having committed the offence under investigation, at (tele)communication tools or computer systems which are regularly

[9] Art. 90*ter* §5 CCP: in case of *flagrant délit* of the terrorism offences mentioned in Art. 137 CC, the taking of hostages (Art. 347*bis* CC), illegal deprivation of liberty (Art. 434 CC) or extortion (Art. 470 CC).

used by this person under suspicion or at places where this person is suspected to be staying or at persons that are deemed, on the basis of precise facts, to regularly be in contact with the suspect; and

(ii) the investigative measure is only justified for a limited list of serious offences (Art. 90ter §§2-4 CCP).

There is **no limitation** as to what **types of data** can be searched.

A **written substantiated order** is necessary. In urgent circumstances, the public prosecutor can orally order the measure, but it needs to be confirmed in writing.[10] When ordering the measure, the competent authority must ensure respect for the proportionality principle, making sure the measure is limited to what is necessary in the light of establishing the truth. The order must contain the information prescribed by art. 90*quater* CCP, including, among others, the reasons for the necessity of the measure[11].

If the investigative measure is applied in real team ('monitoring'), the **duration** of the investigative measure is limited to one month. The investigating judge can prolong the duration one month at a time, for a maximum of six months.[12]

Art. 90*sexies* and 90*septies* CCP provide for specific requirements in relation to **the storing of the information** received by applying the measure provided in art. 90*ter* CCP. The intercepted communication and data should be registered and stored in a file which is stored at the registry. Data which are considered relevant for the investigation should be recorded in separate files, which will be part of the criminal file. In respect of the data deemed irrelevant, a general description of the content and identification of the means of communication or computer system suffices. Each

[10] Art. 90*quater*, § 1, section 3 CCP: within 24 hours as far as the investigating judge is concerned. Art. 90*ter*, § 5, section 2 CCP, however, stipulates that the public prosecutor must confirm the authorization in writing *as soon as possible*.
[11] Art. 90*quater*, § 1, 2° CCP.
[12] Art. 90*quater*, § 1, 4° and 90*quinquies*, first section CCP. This maximum can be extended by two months with a view to installing the necessary technical tools.

file shall contain the subject of the recorded data and the days and hours on which the measure was carried out.

Art. *90octies* CCP provides special rules for mobile devices belonging to **lawyers or doctors** in order to protect professional privilege. The computer system of a lawyer or doctor may only be searched or monitored if they themselves are suspected of having committed or participated in the commission of a criminal offence which is part of the list of art. 90*ter* §2-4 CCP or if precise facts give rise to suspicion that third parties suspected of having committed such criminal offence are using their electronic communication means. Furthermore, the President of the Bar or the representative of the Provincial Medical Association have to be informed of the measure. Information deemed to be covered by professional secrecy will not be included in the official report of the execution of the measure. Moreover, as a general rule, data relating to **journalistic sources** may not be the subject of an investigative measure, nor, therefore, of a covert computer search.

Article 90*novies* CCP contains a delayed duty of **notification** to each person who has been the subject of a covert computer search in accordance with article 90*ter* CCP, as far as his identity or residence can reasonably be established. Said persons must be notified about the nature of the measure applied and the days on which it was implemented and this within 15 days after the end of the judicial inquiry.

b. Mobile device seized

iii. Transparent investigation

Relevant 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.

Applicable rules

If an object (such as a computer system) is deemed to be useful for finding the truth, restitution, forfeiture, protection of civil interests or stopping the commission of a criminal offence, it can be seized. Usually, law enforcement agencies first perform a search and seize whatever they deem relevant for the investigation. However the seizure can precede the search in as far as it is materially difficult or impossible to perform a search on the spot in order to determine what objects or information are/is relevant[13]. This will often be the case when a computer system has to be searched, taking into account the amount of data to be searched through. In those circumstances, the computer system will often be seized in order to allow law enforcement agencies to search through it. The computer system can be returned to the owner/user afterwards. The competent authority to perform the seizure is the authority which has lawfully access to the object/computer system. For instance, when an investigating judge orders a home search, the officers of judicial police performing the search may seize any object they encounter during the performance of the search within the limits of the order and which they deem useful for one of the aims mentioned above. Another example is the search of a suspect. Any officer of judicial police is competent to decide upon and perform such a search. The officer will therefore also be the competent authority to perform a seizure in the framework of such a search.

Once a mobile device has been seized, it can be investigated. We refer to the applicable rules in case of a transparent investigation of a mobile device which is not seized (*supra* title 3.a.i.). The only difference relates to the competent authority. According to art. 39*bis*, § 2 CCP each officer of judicial police can decide to search for computer data which are stored on a computer system that is seized. The competence to bypass security measures or to apply technical measures to decrypt data however still belongs to the public prosecutor (Art. 39*bis*, § 5 CCP). The competence to force the owner/user to unlock the device and the competence to extend the search to linked computer systems (e.g. the Cloud) still belongs to the investigating judge.

iv. Covert Investigation

[13] See Cass. 10 March 1998, AR P.96.0649.N; Cass. 20 November 2001, AR P.00.0548.N.

Relevant scenarios

Mobile devices may be found during a covert sneak and peek operation or other secret investigative measure.

Applicable rules

In case of a classic sneak and peek operation (for instance in a private premise), law enforcement authorities may stumble upon a mobile device. The classic sneak and peek operation may be combined by an IT sneak and peek operation in as far as it is ordered by the competent authority. The sneak and peek operation does not allow law enforcement authorities to copy all data, since seizure is not the aim of the operation. Only a limited copy is allowed ('sample') in order to perform further investigation. If law enforcement authorities however do not have the time to perform the IT sneak and peek on the spot, the law provides for the possibility to take the computer system with them for a strictly limited period of time in as far as the information cannot be obtained by other means (46*quinquies* §5 CCP). The private premise can then be additionally entered to put the computer system back in place. This should be done as soon as possible unless it impedes the proper conduct of the investigation. Therefore, in the framework of an IT sneak and peek, a computer system can be seized (however this seizure will in principle be limited in time) in order to allow the performance of the IT sneak and peek. The applicable rules are the same as those applicable when the system is not seized (*supra* 3.a.ii)).

When law enforcement authorities stumble upon a mobile device when performing a classic sneak and peek operation, the investigating judge may also decide to allow a covert search of the said computer system further to art. 90*ter* CCP. Furthermore, art. 90*ter* CCP also allows the investigating judge to order police forces to secretly enter a private premise in order to get access to a private computer system. In both scenarios art. 90*ter* CCP allows the copying of the data on the computer system (forensic copy), which allows the law enforcement authorities to search through to copied data at a later stage. Taking into account this possibility and the secret nature of the measure provided for by art. 90*ter* CCP, we consider this competence less relevant in relation

to mobile devices which are seized. The mobile device will indeed in principle not be seized in itself when a covert computer search has to be performed.

4. Data kept by a service provider

(answer to question 28)

In principle, law enforcement agencies can also perform a search of computer systems of a service provider. The applicable rules are those mentioned above.

However, Belgian law also contains several cooperation duties which are applicable to (certain) service providers.

The Belgian code on criminal procedure (CCP) provides for

(1) specific cooperation duties for **operators of electronic communication systems and providers of electronic communication services** (which is very broadly defined[14]), to provide (assistance in accessing):

   a. subscriber data (art. 46*bis* CCP) (upon order of public prosecutor)

   b. traffic and location data (art. 88*bis* CCP) (upon order of the investigating judge (and limited competence of public prosecutor in case of *flagrant délit*) and

   c. content (upon order of the investigating judge (and limited competence of public prosecutor in case of *flagrant délit*) (art. 90*quater* §2 CCP);

(2) specific cooperation duties for providers of **financial services and virtual currency exchangers** to provide information on financial products, services or transactions (art. 46*quater* CCP),

[14] Each (legal) person who provides a service or makes a service available on Belgian soil, which consists of the transmission signals via electronic communication networks or which permits customers to the disseminate or receive of information via an electronic communication network.

(3) **general cooperation duties** to assist in the investigation of an IT system or data (art. 88*quater* and 90*quater* §4 CCP), including the duty to search for and provide data. The duty applies to every person/entity deemed capable of providing assistance in the specific matter and has to be ordered by the investigating judge.

The Belgian Code of Economic Law (CEL) furthermore provides for a production order for

(4) **mere conduit providers** (including internet access providers), **caching providers and hosting providers** once it has come to their knowledge that recipients of their services are allegedly committing illegal activities on their networks or servers. The production order can relate to any kind of information which could help the competent LEA in identifying and investigating the infringement (art. XII.20 CEL).

In principle, the service provider can also voluntarily cooperate with law enforcement authorities. However, the service provider will have to make sure its cooperation respects data protection regulations. Without a legal order to provide the data, the service provider might argue that the provision of the data is lawful further to article 6.f GDPR (i.e. processing necessary for the purposes of the legitimate interests pursued by the controller or by a third party). However, this will only be the case in as far as the processing is proportionate and the legitimate interests pursued are not overridden by the interests or fundamental rights and freedoms of the data subject. Voluntary cooperation thus presupposes a balancing exercise for which the service provider is responsible. Cooperation further to a legal order will be deemed lawful further to art. 6 c. GDPR (i.e. processing necessary for compliance with a legal obligation to which the controller is subject), in as far as the provided information is strictly necessary for the fulfilment of the legal obligation.

5. Inadmissibility of evidence

(answer to questions 15 and 30)

Not following the applicable rules does rarely lead to inadmissibility of the evidence in court.

Art. 32 of the preliminary title to the CCP provides that only in three situations exclusion is possible and compulsory:

- if the law explicitly provides nullity for failure to meet a legal requirement;
- if the reliability of the evidence has been tainted; or
- if the use of the evidence violates the right to a fair trial.

Firstly, there is almost no law providing for the sanction of nullity. The sanction is currently only linked to some specific requirements when seizing real estate, when allowing a testimony in full anonymity and when performing a polygraph test.

Secondly, as far as the reliability is concerned[15], we can firstly refer to evidence that is dependent from a person's own free will (witness statements, confessions,...). The reliability of this type of evidence could suffer from illicit pressure or influence from the police. Statements made under those circumstances may conflict with the truth and should therefore be excluded. On the other hand, the evidence that is independent of a person's free will (blood or DNA test, wiretapping,...), can still be unreliable. DNA tests for instance are regulated in detail. A violation of these regulations does not entail nullity, but the fact that the evidence was not collected in conformity with the technical standards, may very well have a negative impact on its reliability. Of course, reliability will also be taken into account when judges assess the probative value of *legally* obtained evidence, but when a legal provision is violated and that violation affects reliability of evidence, the evidence should be excluded.

[15] S. DE DECKER, F. VERBRUGGEN, "Across the River and Into the Poisonous Trees. From exclusion to the Use of Illegally Gathered Evidence in Criminal Proceedings in Belgium", in *The XIIIth World Congress of Procedural Law: the Belgian and Dutch Reports*, Antwerpen, Intersentia, 2008, 76-77.

Thirdly, as far as the violation of the right to a fair trial is concerned, the Supreme Court laid down some guidelines to determinine whether the right to a fair trial is violated or not. According to the Supreme Court, trial judges can, among other things, take into consideration one or more of the following elements: the deliberate or inexcusable nature of the illegal action of the authorities; the seriousness of the offence under investigation when compared to that of the illegal investigative action, the fact that the illegally gathered evidence only relates to the material element of the offence, the fact that the illegality only concerned a formality and the impact of the illegality on the right of freedom protected by the violated norm.

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

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

Belgian law lacks a general framework protecting the reliability and integrity of digital evidence. There is no detailed legal regime on technical requirements regarding the execution of a search of mobile devices nor clear requirements regarding the tools which may be used to perform such searches or processes or adaptations which may be applied to the computer systems under investigation.

Article 39*bis* §8 CCP only stipulates that *suitable technical means* should be used to ensure the integrity and confidentiality of data which are seized and further investigated. Appropriate technical means shall also be used for their preservation at the Registry of the court. A similar provision can be found in the legal framework of covert computer searches. Further to articles 90*sexies* and 90*septies* CCP intercepted communication and data should be registered and stored for further use, for example by the defence. Art. 90*septies* §1 CCP requires the use of *suitable technical means* to ensure the integrity and confidentiality of the registered communications and data and, as far as possible, the translation and recordings of the parts deemed relevant. Guidelines

seem to exist at the level of the public prosecutors' office and police forces but are not accessible to the public.

The technical tools used or adaptations made (such as changing the configuration) only lead to illegally obtained evidence in as far as it can be argued that no '*suitable technical means*' were used as prescribed by law, which will imply a factual discussion. Even if the evidence is obtained 'legally', the use of technical tools, the application of technical processes or the altering of data or the configuration could still lead to discussions in court as to the reliability of the evidence[16]. Lawyers of the defence could indeed try to argue that the changes made to the configuration could alter the content of the data gathered as evidence. In as far as the lawyer's arguments seem plausible, it will be up to the prosecution to convince the judge that the reliability of the evidence is not at stake.

In this regard, it is important to note that Belgium has rather few explicit rules on assessment of evidence. Judges can freely assess the weight of the admissible evidence put before them and are only bound by their "deep-down conviction" *(innerlijke overtuiging – l'intime conviction)*. Specific exceptions to the free assessment of evidence are rare and do not relate to digital evidence. However, this free assessment does not allow the judge to alter the content of the evidence or official reports in the case file.[17]

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

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

See answer to question 31. No specific rules exist in criminal procedure.

[16] Cf. C. CONINGS, *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Antwerpen, Intersentia, 2017, 324; J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime 3.0*, Brussel, Politeia, 2019, 231.
[17] S. DE DECKER, F. VERBRUGGEN, "Across the River and Into the Poisonous Trees. From exclusion to the Use of Illegally Gathered Evidence in Criminal Proceedings in Belgium", in *The XIIIth World Congress of Procedural Law: the Belgian and Dutch Reports*, Antwerpen, Intersentia, 2008, 65.

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

Answer: Indication of length of answer: couple of paragraphs

We understand this question relates to criminal offences (at least partially) committed across borders and in which, mobile devices located in Belgium, may be involved.

The first question is whether Belgian authorities would themselves be competent to investigate the offence:

(i) **Territoriality principle** (art. 3 Criminal Code): according to the main principle, Belgian authorities are competent to investigate a criminal offence as soon as the offence is committed on Belgian territory. According to the *ubiquity criterion*, a criminal offence is committed in Belgium as soon as one of the constitutive elements thereof occurs on Belgian soil.

(ii) **Active personality principle** (art. 6, 7, 9 and 10*quater* §2 preliminary title to the CCP): in some specific circumstances, Belgian authorities will be competent to investigate a criminal offence which is committed abroad by a Belgian or Belgian resident:

- depending on the type of the offence committed (art. 6, 9 and 10quater), or
- in case of double criminality and, if committed against a foreigner, upon complaint of the foreign victim or his family or upon official notice by the foreign country (art. 7).

(iii) **Passive personality principle** (art. 10, 5° and 12 preliminary title to the CCP): in some specific circumstances, Belgian authorities will be competent to investigate a criminal offence of which the victim is a Belgian national. This competence relates to offences punishable under the law of the country where it was committed by a penalty exceeding a maximum of five years' deprivation of liberty.

(iv) **State protection principle** (art. 6 1° and 2° and 10, 1° and 2° preliminary title to the CCP): Belgian authorities will be competent to investigate criminal offences threatening state security.

(v) **Universality principle** (art. 6, 3° *juncto* 10, 3°, 10*ter* and 10*quarter* CCP): in some specific circumstances, Belgian authorities will be competent to investigate criminal offences which are deemed very serious and which therefore justify universal jurisdiction.

When Belgian authorities are competent and decide to investigate the offence, the Belgian rules on investigations of computer systems (*supra*) will be applicable to the investigation of the digital device which is located in Belgium.

When Belgian authorities are not competent to investigate the offence or are not interested to investigate the offence, they can still be asked by a competent foreign authority to assist them during their investigation. The applicable rules depend on the applicable international legal framework. For instance, within the EU, the European Investigation Order (EIO) is the main instrument to ask for cooperation when performing an investigation. It allows an authority in one member state (the "issuing authority") to request all kinds of criminal investigative measures to be carried out by an authority in another member state ("requested authority", here: Belgium). The EIO is based on the principle of mutual recognition, which implies the requested authority will apply local law when executing the investigation and will do this as if it was asked to do so by its own authorities. The requested member will however additionaly take into account procedures and formalities specified by the issuing member state in its request.

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

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

We understand that this question, in contrast to the previous question, relates to the gathering of evidence which is located abroad.

As explained in the first part of this questionnaire, the Belgian legislation is very far-reaching in as far as cross border gathering of digital evidence is concerned. Belgian law allows copying data which are accessed from within Belgian boundaries by means of a transparent remote search or a covert computer search, but which are found not to be situated on Belgian territory. The authorities of the state concerned will be notified, if this state can be reasonably identified. The preparatory works explain that the legislator wanted to enable a unilateral cross border search in order to be able to counter the risk of losing evidence. The preparatory works add, however, that if there is enough time and knowledge, traditional rules on international cooperation should be applied.[18] We doubt whether the traditional rules are even considered in practice given the explicit competence provided by law to copy the data directly. It can furthermore be questioned whether the unilateral cross border search is in conformity with European and international legislation and the principle of state sovereignty[19].

Furthermore, Belgian law is also far reaching as to the possibility to compel foreign service providers to provide cooperation to a Belgian criminal investigation. In principle, service providers providing their services within Belgium, can be ordered directly to comply with a cooperation order of a Belgian authority further to art. 46*bis*, 88*bis* and 90*ter* CCP (*supra*)[20].

In as far as the traditional rules on international cooperation are concerned, the **EIO** is the main legal instrument to be applied when the performance of an investigative measure in a foreign EU country is needed.

The 2000 EU-convention on mutual assistance still applies for evidence gathering not covered by EIO, such as Joint Investigation teams. Two or more member states can set up a **JIT** via a JIT agreement. The JIT is set up with a specific purpose and for a limited time. Each official part of the JIT leads the activities in the territory of its own member state. A JIT can be set up where a

[18] MvT, *Parl. St*. Kamer 1999-2000, 213/1, 24.
[19] C. CONINGS, J.J. OERLEMANS, "Van een netwerkzoeking naar online doorzoeking: grenzeloos of grensverleggend", *Computerrecht* 2013, afl. 1, 27 ff;
[20] See especially: Cass. 1 December 2015, AR P.13.2082.N.

member state's investigation requires difficult and demanding investigations within other member states or where a number of member states are conducting investigations into criminal offences which necessitate coordinated action in the member states involved.

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

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

We refer to the answer to question 34.

Since the EIO Directive is aimed at speeding up cooperation by setting strict deadlines (90 days to act) and at simplifying cross-border criminal investigations in the EU by limiting grounds of refusal and by implementing single standard form, we understand applying this framework is preferable.

Art. 34 of the EIO Directive furthermore provides that the directive replaces the corresponding provisions of the European Convention on Mutual Assistance in Criminal Matters of the Council of Europe of 20 April 1959, as well as its two additional protocols, and the bilateral agreements concluded pursuant to Article 26 thereof; the Convention implementing the Schengen Agreement and the Convention on Mutual Assistance in Criminal Matters between the Member States of the European Union and its protocol.

MLAT-agreements will of course still be applied in relation to states which are not part of the EU. We, however, once again refer to the far reaching unilateral competences provided under Belgian law, as explained in our answer to question 34.

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

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

Except for the existence and application of the cooperation duties which we mentioned in title 4 in the first part of this questionnaire, we are not aware of existing mechanisms and practices. We can however imagine such mechanisms indeed exist.

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

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

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

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

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

Firstly, there are a few principles and rules which are formulated in rather general terms which should be taken into account to avoid discussions in court.

1. **Right to privacy**: Further to art. 8 ECHR each investigative measure which interferes with the private life of individuals should always be applied in a **proportionate** manner.
2. **Data protection law**: The Law Enforcement Directive has been implemented into Belgian law by the second title of the legislative act of 30 July 2018 (Data Protection Act). The

principles enshrined in said second title also apply to the processing of personal data in the framework of a criminal investigation[21], such as:

- **Proportionality principle:** the processing of personal data should always be proportionate and limited to what is strictly necessary.
    - Art. 33, 1° of the Data Protection Act states that the processing is lawful only if and to the extent that the processing is necessary for the performance of a task carried out by a competent authority for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security;
    - Art. 28, 3° of the Data Protection Act states that the personal data should be adequate, relevant and not excessive in relation to the purposes for which they are processed.
- **Accuracy:** Art. 28, 4° of the Data Protection Act states that the personal data should be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.
- **Processing of sensitive data** (art. 34 Data Protection Act): Processing of sensitive personal data (personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation) is only allowed where strictly necessary, subject to appropriate safeguards for the rights and freedoms of the data subject, and only:
    - where authorised by Belgian law, Union law or an international agreement;
    - to protect the vital interests of the data subject or of another natural person; or

[21] C. FORGET, "Protection des données dans le secteur de la "police" et de la "justice"", in V. FRANSSEN, D. FLORE, *Société numérique et droit pénal, Belgique, France, Europe*, Brussels, Bruylant, 2019, 333.

- where such processing relates to data which are manifestly made public by the data subject.

The appropriate safeguards shall provide at least for the competent authority or the controller to draw up a list of the categories of persons having access to the personal data. The competent authority shall ensure that the persons designated are bound by a confidentiality duty.

- **Time limit for storage:**
  - Art. 28, 5° of the Data Protection Act determines that the personal data should be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which they are processed.
  - Art. 30 of the Data Protection Act states that the law should specify the maximum period of time during which the personal data can be retained.

Belgian Criminal Procedure Law does not contain specific rules, further elaborating on these principles, which should be kept in mind when analyzing computer systems or data which are obtained in a lawful manner with respect to the legal provisions as outlined in the first part of this questionnaire. There are for instance no specific rules to guarantee that very sensitive information which is not relevant to the investigation will not be used. The analysis should of course in any case respect the limits as set out by the competent authority (public prosecutor/investigating judge) who ordered the investigative measure.

To our knowledge, very limited case law exists on how the proportionality test can be assured in the context of an investigation of a computer system. In a competition case, the Court of Appeal in Brussels[22] did specify that the search of relevant data should take place by the use of at least two keywords that are sufficiently precise and linked to the subject of the search. The relevance of the outcome should then be tested by way of sampling. The Court also seems to suggest that the analysis should take place in the presence of the accused. The accused should be given sufficient

[22] Brussel 5 March 2013, unpublished, as referred to in Cass. 22 January 2015, AR C.13.0532.F.

time and facilities to oppose against the seizure of data. Information which was not selected as relevant, should furthermore be deleted in the presence of the accused.

As far as the storage of seized data or computer systems is concerned, the seizure should be limited to what is strictly necessary for one of the legal aims of the seizure (*supra*). Depending on the stage of the criminal proceedings, it will be up to the prosecutor, investigating judge or judge to decide upon the termination (or limitation) of the seizure. The law does not provide for a maximum period of time during which the seized computers or data may be kept stored.

In the framework of a covert computer search, the law deviates from the abovementioned limitation principle. Articles 90*sexies* and 90*septies* CCP determine that the intercepted communication and data should be registered and stored for further use. This storage should allow the parties to the proceedings (such as the defence) to get access to the whole set of data in order to enable them to put the data which were selected as relevant within their context. The legislator explicitly decided not to allow destruction of the files with intercepted communication and data, even not after a a certain period of time[23].

As far as the right to a fair trial is concerned, access should be granted to all evidence in the possession of the competent authorities, whether for or against suspects or accused persons, to those persons or their lawyers in order to safeguard the fairness of the proceedings and to allow them to prepare the defence. In more general terms, the prosecution should add all elements to the criminal file which could be relevant for the truth finding.[24] Law enforcement authorities should furthermore be sufficiently transparent about the way they performed their investigation, the results thereof and the further treatment of the evidence encountered. This should allow the parties to the proceedings to check the reliability of the evidence and the legality of the investigation and to raise potential problems before the court. In case of lack of transparency, one could argue that the right

[23] C. CONINGS, *Klassiek en digitaal speuren naar strafrechtelijk bewijs,* Antwerpen, Intersentia, 2017, 224.
[24] Cass. 30 October 2001, AR P.01.1239.N, *Arr. Cass.* 2001, 1815.

to a fair trial has been breached. However, exceptions to this transparency duty are accepted, amongst others to protect police methods (such as technical intelligence)[25].

In this regard, we refer once again to the principle of free assessment of the probative value of evidence put before the court. In as far as the lack of information would allow the lawyers of the defence to cast doubt on the reliability of the evidence, this could not only lead to an argument based on the right to a fair trial, but it could also have an impact on the probative value of the evidence as perceived by the court and on the deep-down conviction of the court. The same is true for an argument based on the potential bias of a tool used.

Section 3: Admissibility of evidence before court

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

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

There are no legislative requirements concerning the treatment of digital evidence once it has been seized and before it is presented in court.[26]

Guidelines however exist[27]. The *Electronic Evidence Guide*, which has been created at the level of the Council of Europe is a basic guide for police officers, prosecutors and judges containing *guidelines* on the handling of digital evidence in all phases of the criminal investigation, prosecution and during trial. It is based on best practices and national and international standards in the countries which are a party to the Cybercrime Convention. The guide is available at https://rm.coe.int/09000016809efd7f. Guidelines also exist at the level of the Public Prosecutor's

[25] ECHR 16 February 2000, n° 28901/95, Rowe and Davis/United Kingdom; ECHR 16 February 2000, n° 27052/95 Jasper/United Kingdom; ECHR 16 February 2000, n° 29777/96, Fitt/United Kingdom; ECHR 25 September 2001, n° 44787/98, P.G. and J.H./United Kingdom; ECHR 27 October 2004, n° 39647/98, Edwards and Lewis/United Kingdom; ECHR 4 April 2017, n° 2742/12, Matanovic/Croatia; C. CONINGS, *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Antwerpen, Intersentia, 2017, 556-558; T. DECAIGNY, *Tegenspraak in het vooronderzoek*, Antwerpen, Intersentia, 2013, 171.
[26] J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime 3.0*, Brussel, Politeia, 2019, 235.
[27] J. KERKHOFS, P. VAN LINTHOUT, *Cybercrime 3.0*, Brussel, Politeia, 2019, 235.

office and at the level of the federal police. However these national guidelines are not accessible to the public. A breach of these guidelines will not render the evidence 'illegal'.

As mentioned before, (electronic) evidence will only be deemed inadmissible if it is illegally obtained and only

- if the law explicitly provides nullity for failure to meet a legal requirement;
- if the reliability of the evidence has been tainted; or
- if the use of the evidence violates the right to a fair trial.

(*supra* p. 25 and 26)

In as far as the electronic evidence is legally obtained, it can be presented before the court. The latter will freely assess the probative value of the data put before it.

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

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

Yes. We refer to our answer to question 38.

As far as discussions on the probative value of the evidence is concerned (cf. free assessment of the court), the volatile nature and ease to change the data will of course have to be taken into account. In case of electronic evidence and mobile forensics, it will be a bigger challenge for law enforcement agencies to show the data have not been altered content-wise while investigating the data (for instance by using forensic tools). Also the chain of custody will therefore, in our view, be more important for electronic evidence.

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

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

Supra p. 25 and 26.

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

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

As explained in the first part of this questionnaire, the Belgian legislation is very far-reaching in as far as cross border gathering of digital evidence is concerned. Belgian law allows copying data which are accessed from within Belgian boundaries by means of a transparent remote search or a covert computer search, but which are found not to be situated on Belgian territory. The authorities of the state concerned will be notified, if this state can be reasonably identified.

Defence lawyers could argue before a court that the unilateral cross border search is breaching European and international legislation and the principle of state sovereignty. However, even if such argument would hold up in court, it will be very unlikely that this would lead to exclusion of the evidence obtained taking into account (i) the fact that a breach of rules on sovereignty does not necessarily render the evidence obtained 'illegal' (see *infra*, our answer to question 46) and (ii) the limited exclusion grounds of art. 32 of the preliminary title of the CCP if the evidence would be considered illegally obtained (*supra* p. 25-26).

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

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

This will once again fall under the free assessment of the probative value of the evidence put before the court. In as far as the alteration would allow the lawyers of the defence to cast doubt on the

reliability of the evidence, this could have an impact on the probative value of the evidence as perceived by the court and on the deep-down conviction of the court. It is therefore important for LEA to be able to show that the alteration did not affect the content of the data they are presenting as evidence in court.

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

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

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.*

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

No, we are not aware of such case law.

***45.* Question:** *Is there in your jurisdiction an established and recognised standardisation(s) of the processes of collection, analysis, interpretation and reporting of digital evidence that must be followed for the evidence to be admissible? (as critical to the validity of evidence, their quality and impact evidence's acceptance by the courts)? If yes, please elaborate.*

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

No, not to our knowledge.

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

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

The question whether evidence is admissible according to art. 32 of the preliminary title of the CCP, raises as soon as the evidence is 'illegally obtained'.

The Supreme Court clearly defined 'illegal evidence' in a 2004 decision.[28] Evidence is considered illegal if it has been gathered (by criminal prosecution authorities or the person reporting the offence who engaged in the illegal action with the purpose of using the data or goods as evidence in a criminal case[29]):

- Through an offence;
- in violation of criminal procedural legislation;
- in violation of the right to privacy (art. 8 E.C.H.R.);
- in violation of the rights of the defence (art. 6 E.C.H.R.) or
- in violation of the right to human dignity.

A violation of data protection law or privacy rules does therefor suffice to raise discussions as to the admissibility of the evidence. However, the evidence will only be excluded in as far as one of the exclusion grounds listed in art. 32 of the preliminary title of the CCP is applicable. Since the data protection and privacy rules do not explicitly provide for nullity in case of a breach, the evidence will only be excluded if the reliability of the evidence has been tainted or if the use of the evidence violates the right to a fair trial (*supra* p. 25 and 26).

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

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

We are aware of only one case in which the admissibility of digital evidence was questioned, in which both the court of first instance and the court of appeal decided upon the issue.

[28] Cass. 23 March 2004, AR P.04.0012.N.
[29] Cass. 17 January 1990, *Arr.Cass.* 1989-90, no. 310.

The case concerned the search of a mobile phone, which had been seized a few weeks before the search was executed. After the seizure and while the search was executed, a connection to an external computer system (chat app) was made involuntarily, which led to the receipt of (and access to) a new message. This new message was the start of a separate criminal investigation.

However, the competent authority did not order the extension of the search of the computer system, meaning the police officers were actually only competent to search the messages which were already stored on the mobile phone. The new message was therefor 'illegally obtained'.

The court of first instance of Antwerp[30] considered that the unlawfulness violated the right to a fair trial, since the unlawfully obtained message triggered the start of a completely new criminal investigation, while one knew or should have known that the said irregularity had occurred. The court also pointed out some other procedural problems in the file, concluding that the procedure as a whole could not be considered to be fair. The illegally obtained evidence, and all the fruit of the poisonous tree, had to be excluded. Because the illegally obtained evidence formed the basis of the entire criminal investigation, the court acquitted the accused.

The court of appeal of Antwerp[31] also decided that the message was illegally obtained. The court however considered that the evidence should not be excluded since (1) the relevant articles of the CCP did not contain a sanction of nullity, (2) the reliability of the evidence had not been tainted and (3) if the use of the evidence did not violate the right to a fair trial. As far as the right to a fair trial is concerned, the court of appeal considered the following:

- The illegal action had not been committed deliberately and was not of an inexcusable nature.
- The illegal action was rather limited and did not outweigh the seriousness of the offence under investigation.

[30] Corr. Antwerp, 11 December 2018, unpublished, as referred to in in K. DE SCHEPPER, "Vrijspraak door schending toepassingsvoorwaarden 39bis Sv.", *Computerr.* 2019, afl. 1, 74-75.
[31] Antwerp 3 june 2020, unpublished.

- The illegally obtained message was only the incentive to start a new investigation, but was not, as such, to be considered as evidence and was not decisive as to the guilt of the accused.
- The message did not relate to communication of the accused. The illegal action did therefor not breach the privacy of the accused.
- The accused is furthermore free to bring his arguments before the court in relation to the illegally obtained message.
- Potential problems in relation to other investigative measures, do not lead to the conclusion that the right to a fair trial has been breached.

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

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

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

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

No, we refer to our answers above in relation to the free assessment of evidence by the court. There are almost no rules on the probative value of evidence in criminal matters (*supra* our answer to question 31).

In as far as deemed necessary or useful, the judge could decide to involve an expert, but this is definitely not a prerequisite. In principle, the judicial expert should be included in the national register of judicial experts (art. 555/6-555/12 Judicial Code). Exceptions do however exist, for instance when no judicial expert with the required expertise and specialisation is available.

The public prosecutor is furthermore always free to involve a professional ('man van het vak') during the investigation. Contrary to the judicial expert, the professional will however not take an oath.

Specifically in relation to investigation of computer systems, the investigating judge has a specific competence to order any person whom he suspects of having a particular knowledge of the computer system under investigation or of services to secure or encrypt data, to provide information (art. 88*quater* §1 CCP). The investigating judge may furthermore order any suitable person to operate the computer system himself or to search for, make accessible, copy, render inaccessible or delete the relevant data (art. 88*quater* §2 CCP). Art. 90*quater* §4 CCP provides for similar competences in the framework of a covert computer search.

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

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

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.*

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

No.

We refer however once again to the – in our view non-critical but rather directing - applicable guidelines (*supra* our answer to question 38):

- The *Electronic Evidence Guide* of the Council of Europe on the handling of digital evidence in all phases of the criminal investigation, prosecution and during trial.
- Guidelines at the level of the Public Prosecutor's office and the federal police. However, as mentioned before, these national guidelines are not accessible to the public.

A breach of these guidelines will not render the evidence 'illegal'.

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

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

No, not to our knowledge. It has to be stressed however, that case law is not systematically published in Belgium, especially case law from courts of first instance and courts of appeal.

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

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

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

No specific rules, guidance or case law exist on how to respect the right to a fair trial specifically in case of evidence extracted via mobile forensics.

As mentioned before, as a general rule and taking into account the principle of equality of arms access should be granted to all evidence in the possession of the competent authorities, whether for or against suspects or accused persons, to those persons or their lawyers in order to safeguard the fairness of the proceedings and to allow them to prepare their defence. In more general terms, the prosecution should add all elements to the criminal file which could be relevant for the truth finding.[32] Law enforcement authorities should furthermore be sufficiently transparent about the way they performed their investigation, the results thereof and the further treatment of the evidence encountered. This should allow the parties to the proceedings to check the reliability of the evidence and the legality of the investigation and to raise potential problems before the court. In case of lack of transparency, one could argue that the right to a fair trial has been breached. However, exceptions to this transparency duty are accepted, amongst others to protect police methods (such as technical intelligence)[33].

[32] Cass. 30 October 2001, AR P.01.1239.N, *Arr. Cass.* 2001, 1815.
[33] ECHR 16 February 2000, n° 28901/95, Rowe and Davis/United Kingdom; ECHR 16 February 2000, n° 27052/95 Jasper/United Kingdom; ECHR 16 February 2000, n° 29777/96, Fitt/United Kingdom; ECHR 25 September 2001, n° 44787/98, P.G. and J.H./United Kingdom; ECHR 27 October 2004, n° 39647/98, Edwards and Lewis/United Kingdom; ECHR 4 April 2017, n° 2742/12, Matanovic/Croatia; C. CONINGS, *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Antwerpen, Intersentia, 2017, 556-558; T. DECAIGNY, *Tegenspraak in het vooronderzoek*, Antwerpen, Intersentia, 2013, 171.

Furthermore, as far as covert computer searches are concerned, Art. 90*sexies* and 90*septies* CCP provide for specific requirements in relation to the storing of the information received by applying the measure provided in art. 90*ter* CCP. The intercepted data should all be registered and stored in a file which is stored at the registry. Data which are considered relevant for the investigation should be recorded in separate files, which will be part of the criminal file. The storage of the data which are deemed irrelevant should allow the defence to put the data which were selected as relevant within their broader context. This requirement on the storing of the intercepted data is therefor aimed at ensuring the right to a fair trial and equality of arms.

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

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

No. Trainings are not required by law.

In practice, trainings are however provided in a more or less consistent manner for prosecutors and judges. Trainings for lawyers are very limited and mainly focus on legal aspects rather than on technical aspects.

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

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

No.

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

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

Prosecution:

1. **Leading the criminal investigation**: as explained above (*supra* p. 7 and 8), the Belgian investigative stage of criminal proceedings is mainly inquisitorial. Two types of pre-trial investigations can be distinguished: the preliminary inquiry and the judicial inquiry. A preliminary inquiry is led by the public prosecutor, while a judicial inquiry is led by an (impartial and independent) investigating judge. The prosecution thus leads the investigation in case of a preliminary inquiry. During a judicial investigation, the prosecution can still request the investigating judge to perform specific investigative measures. In case of refusal, an appeal can be brought before the Indictment Chamber.
2. **Bringing prosecution:** in case of a preliminary inquiry, the prosecution can decide to prosecute or drop the case. In case of a judicial inquiry, the case will in principle be brought before the council chamber, which will decide whether the case has to be brought before the criminal court. It is no longer up to the prosecution to drop the case. The prosecution can however ask the council chamber to dismiss the case. The prosecution can also propose to solve the case out of court (by way of settlement or criminal mediation).

The trial court:

1. **Rather passive role, deciding upon the case:** the court will hear the parties to the proceedings and will have access to the criminal file. In most case, the court will decide upon the case based on the file which is brought before the court and the arguments which are elaborated in the submissions and pleadings of the parties. If an argument is raised as to the illegality of evidence obtained, the court will be competent to decide upon exclusion of said evidence from the debates in as far as one of the grounds of art. 32 of the preliminary title to the CPP applies. In case of out of court settlements, the court will also have to validate the settlement in as far as a judicial inquiry was initiated or in as far as the case was already brought before the court.

2. **Possibility to perform additional investigative measures:** the court is competent to decide upon the performance of some additional investigative measures. For instance, if the suspect is present during trial, the judge may (and most often will) interrogate the suspect. The judge may also hear a witness. However, for doing so, he will be dependent upon the initiative of one of the parties to the proceedings since he does not have the right to call a witness himself. The court does have the right to appoint an expert.

The defendant

1. **Right to request access to the criminal file:** As a general rule, the defendant will have access to and may copy the criminal file at least once it is brought before the court (the trial court in case of a preliminary investigation and council chamber in case of a judicial investigation). However, when the criminal investigation is still ongoing, the defendant can ask the competent authority (public prosecutor/investigating judge) to have access to the criminal file and to obtain an authorisation to copy the criminal file (art. 21*bis* and 61*ter* CCP). The public prosecutor or investigating judge may refuse access or taking of a copy of the file or of certain documents if, amongst others, the necessities of the investigation so require or if access would endanger persons or seriously harm their privacy or if the applicant shows no legitimate reason for consulting the file. The public prosecutor or investigating judge may also restrict access or the taking of a copy to that part of the file in respect of which the applicant has an interest. In as far as access to the criminal file is refused, appeal will be possible before the Indictment Chamber. Seized material or data, which are most often stored at the registry, are also and under the same conditions accessible for the defendant.
2. **Right to request additional investigative measures:** the defendant has the right to add all information or documents which he deems relevant to the criminal file. During a preliminary investigation, he can suggest to the prosecution to perform additional investigative measures. However he does not have a right to formally request such additional investigative measures. During a judicial investigation, the defendant has an

explicit right to request additional investigative measures (art. 61*quinquies* CCP). The investigating judge may refuse this request if he does not consider the measure necessary to establish the truth or if, at the time, he considers that the measure is prejudicial to the investigation. In case of refusal, appeal will be open before the Indictment Chamber.

3. **Right to request the lifting of a seizure:** Both during a preliminary inquiry and judicial inquiry, the defendant has the right to request the competent authority (prosecutor/investigating judge) to lift a seizure (art. 28*sexies* CCP and art. 61*quater* CCP). The right actually belongs to every person who is harmed by an investigative measure which is performed in relation to his/her goods. The competent authority may reject the request if he considers that the necessities of the investigation so require, if the rights of the parties or third parties would be adversely affected by the lifting of the seizure, if the removal of the act would endanger persons or property, or if the law provides for the return to the rightful owner or the confiscation of the property in question. The competent authority may also authorise a partial or conditional lift. Appeal is possible before the Indictment Chamber.
4. **Right to adequate time and facilities to prepare defence:** once the case is brought before the court, the defendant will have the right to adequate time and facilities to prepare his defence. The defendant will be given access to the criminal file and will be given time to prepare written arguments. The defendant can request additional investigative measures, such as the interrogation of a witness, but the court is not obliged to grant this. If the defendant is present in person during trial, he will in principle be heard by the trial court.

The victim

1. **Right to initiate criminal proceedings:** the victim has the right to initiate criminal proceeding by summoning the suspect before the criminal court (in case of an infraction or misdemeanour) or by filing a civil complaint with the investigating judge (in case of a misdemeanour or crime). In both scenarios, the victim will be a 'civil party' to the proceedings. The victim can also decide to file a complaint with the police or public

prosecutor's office. The latter could however decide to drop the case. Once a preliminary investigation is started, the victim can also make a declaration of injured party. As injured party, the victim will be kept informed about a decision to drop the case, a decision to start a judicial investigation or a decision to bring the case before the court.

2. **Right to request access to the criminal file:** once the victim has the capacity of *civil party* or of *injured party*, he will have the same rights to access the criminal file as the defendant (*supra*).
3. **Right to request additional investigative measures:** the victim is free to add all information or documents which he deems relevant to the criminal file. During a preliminary investigation, he is free suggest to the prosecution to perform investigative measures. During a judicial investigation, the victim will have the same rights to request additional investigative measures as the defendant (*supra*), but only once he has the capacity of *civil party*.
4. **Right to request the lifting of a seizure:** As is the case for the defendant, the victim has the right to request the competent authority (prosecutor/investigating judge) to lift a seizure by which he considers himself to be harmed in relation to his goods (*supra*).

The witness

1. **Specific possibilities to protect a threatened witness:** the CPC provides for several protective measures which can be applied for threatened witnesses (art. 102 and further CCP). The most severe measures can only be applied during an investigation into serious offences or offences committed in the framework of a criminal organisation.
2. **Possibility to testify anonymously:** this has to be allowed by the investigating judge and is only possible under very strict circumstances.
3. **Right to request access to the criminal file:** a witness will be considered a third party to the proceedings. Third parties have the right to request the public prosecutor to get access to the criminal file (art. 21*bis* CCP). The public prosecutor is not obliged to give access and

no appeal can be brought against a refusal of the public prosecutor to grant access to the criminal file.

4. **Right to request the lifting of a seizure:** As is the case for the defendant and the victim, a witness has the right to request the competent authority (prosecutor/investigating judge) to lift a seizure by which he considers himself to be harmed in his goods (*supra*).
5. **Before the trial court:** in principle, a witness will be heard during the investigation phase and an official report will be drafted in relation thereto. The trial court will have access to said official report, since it will be part of the criminal file. The witness will therefore in principle not be heard again before the trial court. However, parties have to right to ask the court to hear a witness. The court is however not obliged to agree thereto, but it will have to consider such request in light of the rights of defence and equality of arms.

5.1 The Prosecution

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

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

Next to the legal framework, explained in our answers to the questions above and especially the first part of this questionnaire, only (non-binding) guidelines exist, as explained in our answer to question 38 and 50.

5.2 The Court

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

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

The general legal framework applies.

In as far as an investigation measure belongs to the competence of an investigating judge, the latter will control the acquisition, collection and analysis of the evidence in the framework of the said investigative measure. When a judicial inquiry has been initiated, the investigating judge will furthermore lead this investigation and will control the collection and analysis of the evidence in the framework of this investigation.

In as far as a judicial inquiry has been initiated, the investigation courts (Council Chamber and Indictment Chamber) will also be competent to control whether the evidence was obtained in a lawful manner. The Council Chamber will review the case upon the closure of the investigation. The accused will have the opportunity to argue why certain evidence should be deemed illegal and should be excluded from the file; The Indictment Chamber is the appellate court vis à vis the decision of the Council Chamber. It furthermore has some specific competences during investigation, for instance in case of lengthy investigations. When exercising those specific competences, the Indictment Chamber is also competent to decide on the exclusion of illegally obtained evidence, further to art. 32 of the preliminary title of the CCP.

Once the case is brought before the trial court, this court will also be competent to control whether the evidence was obtained in a lawful manner and to decide upon the exclusion of illegally obtained evidence. The trial court will furthermore be free to assess the probative value of the evidence presented before it. This is the case for both the court of first instance and the court of appeal.

The court of cassation (supreme court) will only perform a judicial control, meaning it will only check whether the law has been respected and applied correctly by the court of appeal (or Indictment Chamber). The supreme court will not assess the facts of the case.

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

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

As explained above, this is part of the free assessment by the trial judge of the probative value of evidence presented before the court.

5.3 The defendant and defender

***59.* Question:** *Are there rules and standards regulating the defendant and his/her defender's rights to access and to make copies of the acquired mobile evidence? Are they able to get any information on the process used to acquire mobile forensic evidence (e.g. information on how the tools work, the procedures used, the parties involved and how the validity of the results is guaranteed)? Please refer to case law if possible.*

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

As mentioned before, as a general rule access should be granted to all evidence in the possession of the competent authorities, whether for or against suspects or accused persons, to those persons or their lawyers in order to safeguard the fairness of the proceedings and to allow them to prepare their defence. In more general terms, the prosecution should add all elements to the criminal file which could be relevant for the truth finding.[34] Law enforcement authorities should furthermore be sufficiently transparent about the way they performed their investigation, the results thereof and the further treatment of the evidence encountered. This should allow the parties to the proceedings to check the reliability of the evidence and the legality of the investigation and to raise potential problems before the court. In case of lack of transparency, one could argue that the right to a fair trial has been breached. However, exceptions to this transparency duty are accepted, amongst others to protect police methods (such as technical intelligence)[35].

[34] Cass. 30 October 2001, AR P.01.1239.N, *Arr. Cass.* 2001, 1815.
[35] ECHR 16 February 2000, n° 28901/95, Rowe and Davis/United Kingdom; ECHR 16 February 2000, n° 27052/95 Jasper/United Kingdom; ECHR 16 February 2000, n° 29777/96, Fitt/United Kingdom; ECHR 25 September 2001, n° 44787/98, P.G. and J.H./United Kingdom; ECHR 27 October 2004, n° 39647/98, Edwards and Lewis/United Kingdom; ECHR 4 April 2017, n° 2742/12, Matanovic/Croatia; C. CONINGS, *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Antwerpen, Intersentia, 2017, 556-558; T. DECAIGNY, *Tegenspraak in het vooronderzoek*, Antwerpen, Intersentia, 2013, 171.

As a general rule, the defendant will have access to and may copy the criminal file, at least once the case is brought before the court (the trial court in case of a preliminary investigation and council chamber in case of a judicial investigation). Also during the criminal investigation, the defendant can ask the competent authority (public prosecutor/investigating judge) to have access to the criminal file and to get an authorisation to copy the criminal file (art. 21*bis* and 61*ter* CCP). When a party to the proceedings requests access to the criminal file, the public prosecutor or investigating judge may refuse the access or taking of a copy of the file or of certain documents if, amongst others, the necessities of the investigation so require or if access would endanger persons or seriously harm their privacy or if the applicant shows no legitimate reason for consulting the file. The public prosecutor or investigating judge may also restrict access or the taking of a copy to that part of the file in respect of which the applicant has an interest. Seized material or data, which are most often stored at the registry, are also and under the same conditions accessible for the defendant.

The criminal investigation phase is typically written in nature. LEA will therefor draw up official reports in relation to the investigation measures they perform. Belgian law however lacks general legislative provisions on what information should be included in the official report[36]. It is advisable however to include as much information as possible in order to avoid discussions in court as to the integrity, authenticity and reliability of the evidence brought before the court.

Specific rules apply in as far as covert computer searches are concerned.

As explained before, art. 90*sexies* and 90*septies* CCP provide for specific requirements in relation to the storing of the information received by applying the measure provided in art. 90*ter* CCP. The intercepted data should all be registered in a file which is stored at the registry. Only the relevant parts of the data will be included in official reports in the criminal file. Specific rules apply to get access to the data stored at the registry:

[36] C. CONINGS, *Klassiek en digitaal speuren naar strafrechtelijk bewijs*, Antwerpen, Intersentia, 2017, 360-361; T. DECAIGNY, *Tegenspraak in het vooronderzoek*, Antwerpen, Intersentia, 2013, 361.

- The defendant will upon a simple request get access to the recorded data of which certain parts were considered relevant by LEA and are therefore included in an official report to which the defendant has access.
- The defendant may furthermore request the competent judge to get access to the other intercepted data deposited at the Registry and to copy additional parts of the said data and add them to the criminal file. The Judge may reject the request if he considers that the consultation or the transfer or representation of additional parts is not necessary to establish the truth, if he considers it prejudicial to the investigation, or for reasons relating to the protection of rights or interests of other individuals. He may also limit the consultation or copying of additional data.

In as far as the investigating judge ordered a third party to cooperate, further to art. 88quater CCP or 90quater CCP or in as far as an expert was involved, the identity of the third party or expert will appear from the cooperation order or decision to involve an expert.

5.4 Witnesses

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

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

Taking into account the objective of this questionnaire, we understand this question as relating to the protection of privacy of a witness if a mobile device of a witness would be searched or if a mobile device of another person (such as a suspect) would be searched which would contain private information of a witness.

In relation to open computer searches, it should be mentioned that non-relevant data will in principle not be included in the criminal file. Mobile devices which are seized and searched, but which do not appear to contain relevant information nor qualify for confiscation, should in principle be returned to the rightful owner/user. The witness will also have the right to request the lifting of the seizure under the conditions mentioned above (*supra* our answer to question 55).

When a party to the proceedings requests access to the criminal file or seized goods during a criminal investigation (art. 21*bis* and 61*ter* CCP), the prosecutor or investigating judge may refuse the access or taking of a copy of the file or of certain documents if, amongst others, such access would seriously harm the privacy of a person. The public prosecutor or investigating judge may also restrict access or the taking of a copy to that part of the file in respect of which the applicant has an interest.

Once the case is brought before the council chamber or trial court, parties to the proceedings will however get access to the criminal file and goods which are still under seizure. The law does not contain specific provisions limiting the right to access to protect the privacy of parties involved or third parties.

In relation to the IT sneak and peek, it should be mentioned that this measure is not aimed at seizing data.

Covert computer searches can only be applied to investigate the computer system of (or in use by) a suspect (of a serious criminal offence) or a regular contact of the suspect. Furthermore only the relevant parts of intercepted/recorded data will be included in official reports in the criminal file. As mentioned in our answer to question 59, parties will get access to the data which are the broader context of the parts which are considered relevant upon a simple request. Access to other data can be requested but can be refused amongst others for reasons relating to the protection of rights or interests of other individuals.

To our knowledge, there are no particular requirements for witnesses regarding their capability to testify in terms of mobile forensics. As far as judicial experts are concerned, we refer to our answer to question 48.

5.5 The Victim

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

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

Victims can become party to a criminal proceeding by taking the position of a civil party to the proceedings (*supra* our answer to question 55). They can take this position before an investigating judge (by filing a complaint with the investigating judge during a judicial investigation or by which such investigation is launched) or before the council chamber or trial court. During a preliminary investigation, a victim can make a declaration of an injured party.

Both in its capacity as injured party or civil party, the victim will have the same rights to access the file as the accused/defendant (art. 21*bis* and 61*ter* CCP). Both the defendant and victim will be able to request access to the file during the investigation phase. The public prosecutor or investigating judge may refuse the access or taking of a copy of the file or of certain documents if, amongst others, the necessities of the investigation so require or if access would endanger persons or seriously harm their privacy or if the applicant shows no legitimate reason for consulting the file. The prosecutor or investigating judge may also restrict access or the taking of a copy to that part of the file in respect of which the applicant has an interest.

The defendant and victim will in any case get access to the file once the case is brought before the council chamber or trial court.

In the framework of a judicial investigation, both the civil party and defendant will also have the opportunity to request the investigating judge to perform additional investigative measures (art. 61*quinquies* CCP). They could thus for instance request the search of a mobile device. The investigating judge may reject this request if he does not consider the measure necessary to establish the truth or if, at that time, he considers that the measure is prejudicial to the investigation.

The victim will furthermore have a right to request the lifting of a seizure under the conditions mentioned above (*supra* our answer to question 55).

During the trial phase, the civil party can use the evidence obtained via mobile forensics when proving the commission of an offence and the causing of harm.

Taking into account the objective of this questionnaire, we understand the question in relation to the protection of privacy as relating to the situation in which a mobile device of a victim would be searched or if a mobile device of another person (such as a suspect) would be searched which would contain private information of the victim. We refer to our answer to question 60 in relation to the protection of the privacy of witnesses. We are not aware of specific rules aimed at protecting the privacy of victims in the framework of mobile forensics.

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.

/

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

General disclaimer

Answers provided in this questionnaire shall provide general guidance but do not substitute individual legal advice. Our assessment in this questionnaire is based on our analysis of Belgian law and our professional experience. The Belgian legislation concerning the search of mobile devices is relatively new. To the extent that the law does not provide a clear guidance and/or no clear practice has been established yet with respect to the interpretation of certain legal provisions, our assessment is based on the legislative purpose and the spirit of the law rather than on the word-by-word interpretation of a law (which, in certain cases, may even lead to an unreasonable result). We therefore cannot exclude that a Belgian court or other authority would take positions that deviate from what we expressed.