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

IMPORTANT TO READ BEFORE ANSWERING THE QUESTIONNAIRE:

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

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

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

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

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

As we want to be able to compare answers across jurisdictions, we have drafted this request for information in a questionnaire format. This, however, does not mean we are looking for simple yes/no answers. Most questions are open questions and naturally invite an elaborate answer. Some questions may perhaps in theory be answered as yes/no question, but **please give as much 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**

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

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?*

Dr Gavin Robinson

Postdoctoral researcher: Criminal law & IT law.

Faculty of Law, Economics and Finance at the University of Luxembourg.

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

Main headquarters: Belval, Esch-sur-Alzette, Luxembourg.

Faculty of Law, Economics and Finance: Kirchberg, Luxembourg City, Luxembourg.

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

There is no such legally-defined term. Nor is there any tailored regulation of digital devices or evidence in general in Luxembourg criminal procedural law. For instance, the seizure provisions, applicable both to mobile devices and to data on mobile devices, are very broadly-termed (Arts 33 & 66 of the *Code de procédure pénale* – Code of Criminal Procedure – 'CPP').

Preliminary note: with very rare exceptions, the law, all jurisprudence, as well as commentary and doctrine in Luxembourg (at least on domestic legal issues) is only available in French. All translations in this report are the author's own, and are thus entirely non-official.

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

Section 1: Criminal procedure when searching/reading mobile devices, seizing mobile devices and for acquisition of data on mobile devices

Question: *Mobile devices (e.g. a smartphone) may enter investigations in a variety of scenarios. A suspect or a witness may have a smartphone on them during questioning or at the scene, mobile devices may be found during the search of a home or other premises, a suspect caught in the act may have a mobile device in use etc. We want to know for all these scenarios (and others you may be able to identify) what the applicable national rules are, namely answering the following questions:*

Mobile device not seized

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

The powers of seizure (by the judicial police in limited circumstances, otherwise by the investigating judge) set out in the CPP apply to both mobile devices and to the data stored on them. Whilst the former scenario (seizure of *devices*) is dealt with in a separate section below, the latter (where *data* alone are seized) seems to fit here: a mobile device being read or searched before data is seized therefrom – even if the precise demarcation between "search" and "seizure" may at times be difficult to draw in practice.

An express reference to data was inserted into the CPP provisions by the Law of 18th July 2014 (implementing the Budapest Convention; Mémorial A133) where none had previously existed; until then, the seizure of data was nonetheless carried out in practice on the basis of the existing texts, despite their unequivocal emphasis on physical objects. Since that reform, it is established in the CPP that seizure of data can be done either by taking possession of a device (*support physique*) or by making a copy of the data made in the presence of the persons attending the search (art. 66(3) CPP). The express possibility to copy data in the context of a seizure was inserted in the CPP by the 2014 reform in order to tackle the complexities involved in seizing immaterial data effectively and proportionately. For instance, where the targeted data are stored on a server along with the data of other persons who are not the subject of the judicial order, seizing the entire server would impact third parties. Furthermore, the sought data might be found on the device of an "operator" who is not targeted by the preliminary investigation or judicial inquiry. Being able to make a copy of the data means there is no need to seize the object of a third party (necessitating in turn a fresh investigation or *instruction*). In certain cases, in particular concerning small businesses, in practice the copying of data may be preferred to seizure of devices where the latter would simply paralyse

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

operations. Lastly, servers may often be so large as to "fill entire rooms", rendering physical seizure of hard disks impossible (see the Bill for the Budapest reform: *Projet de loi* n° 6514, *Rapport de la commission*, p.12).

If a copy is made, the investigating judge may order the definitive erasure of the data on the device, where the device is located in Luxembourg and is not "in the hands of justice", where possession or use of the data is illegal or dangerous for the security of persons or goods (Art. 66(3), CPP). By doing so, the further commission of various cybercrime offences can be prevented – from hacking offences to possession or distribution of illegal content such as child sexual abuse material. What is perhaps not immediately apparent from the wording of the provision is that in order to erase data, a copy *must* first be made. Apart from facilitating future use of the data as evidence, the existence of a copy is required in case the erasure decision is successfully challenged before the pre-trial chamber or at trial, or in case proceedings are discontinued or end in acquittal. Should no copy of (legal) data remain, its restitution would be impossible. In practice, it is reported by prosecutors that when a copy of seized data is made, in general the data are saved on a CD, DVD or hard drive, or even (less secure) USB sticks depending on the volume of data to be seized (Respectively *Rapport d'évaluation sur le septième série d'évaluations mutuelles "Mise en œuvre pratique et fonctionnement des politiques européennes en matière de prévention de la cybercriminalité et de lutte contre celle-ci" – Rapport sur le Luxembourg (Brussels, 19th May 2017),* ('GENVAL Evaluation') at 49. Available at http://data.consilium.europa.eu/doc/document/ST-7162-2017-REV-1-DCL-1/fr/pdf and Putz (2019), p. 264. These sources do not however mention device type.

All of the provisions set out so far do apply to mobile devices. Naturally, however, several of the points made in the foregoing are less pertinent in respect of mobile devices (which tend to be more for personal, individual or family use) than of businesses' or law firms' computer networks, servers or data centres, etc. Indeed in practice it would seem to be the norm that physical mobile devices (especially mobile telephones) are simply seized rather than undergoing data extraction/analysis at the place or site of seizure – and far less when suspects are stopped and searched in public. Although search (*perquisition)* and seizure (*saisie)* are independent acts, each with dedicated rules in the CPP, the principal goal of a "real-world" search (further explained in Q5) is to allow the seizure of devices (Putz, 2019, pp.242-243). Alongside searches (*perquisitions*: of domiciles, offices, vehicles etc), bodily searches (*fouilles corporelles*) by the police often turn up mobile telephones – which, if obtained legally, can be added to the *dossier* (case file). Grounds for performing a bodily search are set out in Q5.

In the less likely event that a mobile device is not seized for later analysis (by agents of a specialised internal police "support" unit, the *Service de Nouvelles Technologies*, SNT), there remains the question of what can lawfully be done on that device at the site of a search, prior to any seizure. This is not specifically regulated in Luxembourg law, and no commentary seems to hint at such operations taking place on mobile devices, which rarely if at all mentions "search" without "seizure" (Putz 2019, Kraus 2017). Nonetheless, the discussion around accessing and seizing *data*

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

accessible from IT equipment at the search site would also seem potentially relevant to mobile devices (see answer to Q13).

(Including in case relevant): Articles 88-1 to 88-4 CPP set out a series of special measures enabling surveillance of all forms of communications, strictly by the investigating judge in the course of a judicial inquiry. These are the interception of telecommunications and postal correspondence, and since the Law of 27 June 2018 (Mémorial A559)[1] which purposely mirrored developments in France and Belgium (*Exposé des motifs, Projet de loi n. 6921,* p. 7) the making of sound and video recordings in places or vehicles, and the "capture" of IT data. With regard to interception and "data capture", the cooperation of service providers – where needed – is mandatory: "Any person who refuses to provide his technical assistance to the execution of orders referred to in this article is punished with a fine of 1,250 to 125,000€" (Art. 88-4, CPP). The interception ("*surveillance et contrôle"*) of telecommunications is available to the investigating judge in relation to the prosecution of all offences carrying a maximum sentence of at least 2 years' imprisonment. The "capture" of IT data is limited, by contrast, to crimes and misdemeanours against state security, acts of terrorism and terrorist financing. In the case of both powers, there must be clear indications ("*faits déterminés*") which render the person to be surveilled "suspect of either having committed the offence or having participated in its commission, or of receiving or transmitting information intended to reach the *inculpé* or suspect or which come from him" (Art. 88-2(2)2°, CPP).

In light of the breadth of this investigative net and the intrusiveness of the measures in question, the decision of the investigating judge may only order them exceptionally and via a written and detailed decision (*"decision spécialement motivée"*) including – on pain of nullity – reference to the elements of the case, the name or description of the target, the manner in which the measures are to be executed, the name and grade of the judicial police officer executing them, and the duration of the measures. On this last point, the measures must cease as soon as they are no longer necessary, and in any case after one month (extendable monthly up to a total of one year, subject to the approval of the president of the pre-trial chamber of the court of appeal; Art.88-2(3)-(4)). Art. 88-1(3) provides that the "capture" of electronic data "consists in the placement of a technical device with the aim of accessing, without the consent of the persons involved, in any place, electronic data and recording, preserving and transmitting them, as they appear on a screen for the user of a system of automatic processing or transmission of data, as the user introduces them by inputting characters or as they are received and emitted by audiovisual peripheral devices". A similar clause to that discussed above in relation to seizures provides that any person deemed to have the requisite technical knowledge may be ordered by the investigating judge to

[1] The main changes in the 2018 reform are: a more flexible extension of 24-hour detention; undercover online investigations ("*enquête sous pseudonyme par voie électronique")*; searches of premises at any time of day or night; placement of devices in private premises in order to carry out audio or visual surveillance.

(confidentially) assist him in matters of access to and decryption and comprehension of targeted data (art. 88-4(1), CPP).

Other than the provisions on seizure of data from mobile devices and the "special" investigative measures just set out, no powers in the legal framework seem to fit the wording of the question. Whilst Articles 48-12 *et seq* give the investigating judge powers to carry out "systematic observation" with the aid of "technical means", the language in the provisions clearly refers to the observation of physical spaces (domicile or professional premises) by cameras and microphones. It would be impossible to interpret this power to cover cyberspaces (Putz, 2019, p. 237). Moreover, unlike several of its neighbours in Luxembourg there is no power to conduct remote 'digital searches' (*perquisitions informatiques;* in Germany, *Online-Durchsuchung*) which could target mobile devices. In the absence of any provision in the CPP and given the impossibility of respecting even common law rules on search and seizure (for instance, the presence of the target or of witnesses – which seems impossible to arrange in an online setting), in Luxembourg such measures are not only considered illegal in a procedural sense but are also likely constitute a criminal offence of fraudulent access and/or deployment of spyware, depending on the facts (Putz, 2019, p.244).

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?*

The point of departure is that the key operative provisions in the CPP empowering police and judicial actors are conceived to be exceptions to the constitutional baseline of the inviolability of the home (*domicile*) unless prescribed by law (Article 15, Luxembourg Constitution) and the confidentiality of all communications (Article 28, Luxembourg Constitution, reinforced and modernised by provisions of the *Code pénal* (Criminal Code, esp. Article 509-3(2)) and in other secondary legislation, including the implementation of the ePrivacy Directive.

The pre-trial chambers of the "instruction courts" have underlined that any search "must have as its goal to seek and discover objects which are necessary or useful to the *manifestation* of the truth and as such may only take place in order to corroborate pre-existing evidence or indications of a defined offence (*délit*) which is already known and presumed to have been committed and in no case may a search be carried out in order to seek *délits* or *crimes* or hints thereof" (TA Lux, ch. cons., 14 novembre 2018, no. 1983/18 ; TA Lux., ch. Cons., 28 juillet 2017, no. 1724/17).

The police are empowered to carry out bodily searches (all police; art. 39(7) CPP) and searches of vehicles (judicial police only and vehicle in public spaces only; art. 48-10 CPP) upon suspicion that an individual is withholding "objects" which are useful to the discovery of the truth or may be dangerous to that individual or to others (bodily search) or where the driver, owner or a passenger

gives a reason for the judicial police officer to suppose that the former has committed a *crime* or a *délit* (ie. *contravention* is not enough). Otherwise, classic searches (*perquisitions:* of a domicile, professional premises, vehicles) may only be carried out by judicial police officers in case of *flagrant délit* (art. 33 CPP) or when ordered by an investigating judge (art. 65 CPP).

In urgent cases of *crime* or *délit flagrant,* meaning primarily when suspects are caught in the act of committing an offence or in the immediate aftermath (art. 30, CPP), but potentially greatly extendable in the context of a continuous crime (*infraction continue*) giving rise to a permanent state of "flagrancy" (see e.g. Ch. c. C. (*Chambre du conseil de la Cour d'appel*), 2 June 2014, N° 371/14) an officer of the judicial police may seize electronic devices or data as he would any object or document, subject to the essentially the same procedural steps regarding the making of copies and the deletion of data as outlined above in relation to a seizure ordered by the investigating judge. This power is available in relation to all *crimes* and to felonies (*délits*) which carry the sanction of imprisonment (art. 40, CPP). In light of the broad scope and intrusiveness of the measure, which depends heavily on the subjective assessment of police officers, since 2006 Article 48-2 CPP provides that the public prosecutor as well as any person demonstrating a legitimate personal interest may request the annulment of (any act of) the preliminary investigation. This *ex post* judicial review – available on simple request – of preliminary investigations was introduced in order to protect the rights of those involved as well as to ensure early judicial scrutiny of investigative acts undertaken by the police that often lead to the opening of a judicial inquiry (*Projet de loi n°5354,* 30 June 2004, at 19). In the course of an interview with the SNT (Judicial police), I was informed that in practice an investigating judge is systematically alerted by telephone before seizures are carried out (no specification of devices or data). In fact, in Luxembourg a system is in place ensuring that an investigating judge is available on call 24/7 partly in order to cater for such eventualities.

In the usual scenario, therefore, an investigating judge has ordered a search (and seizure). Necessity and proportionality requirements are inherent firstly in constraints placed on the relevant actors i.e. the investigating judge or public prosecutor. Most importantly, the investigating judge (who has a near-monopoly on coercive measures) has the duty to use her powers (so long as the investigating judge is "seized" correctly by the Public Prosecutor, she is obliged to carry out *actes d'instruction;* Ch. c. C., 9 July 2013, n° 375/13) – such as searches and seizures – in order to "discover the truth", meaning in a scrupulously even-handed manner (*à charge et à décharge*; art. 55(1), CPP). Although her freedom to exercise her powers are in principle subject to no restriction, some objective procedural limits are in place; for example, other than in urgent cases of *infraction flagrante* or for a handful of terrorism-related crimes, searches must not take place after midnight and before 6am, on pain of nullity (art. 65(3), CPP).

Whilst a search warrant need only indicate the goal of the search, this must not be so broad as to indicate that the investigating judge did not consider whether less intrusive measures would have sufficed. Luxembourg was notably held in 2013 to have violated Articles 8 and 10 of the ECHR

after a police-only execution on journalists' offices of a search warrant which indicated, *inter alia,* "any documents and items, in whatever form and on whatever medium, connected with the offences charged." Although the investigating judge had of his own motion ordered the discontinuation of the seizure and the return of all documents and items seized during the search, his order was nonetheless subsequently upheld successively by both pre-trial chambers, before an application to Strasbourg was made. In *Saint-Paul Luxembourg S.A. v. Luxembourg*, 18 April 2013, applying the "most careful scrutiny" due for limitations on the confidentiality of journalistic sources, the ECtHR considered that "the impugned search and seizure were disproportionate inasmuch as they enabled the police officers to search for the journalist's sources. The Court notes that the insertion of a USB memory stick into a computer is a procedure which can facilitate the retrieval of data from the computer's memory, thus supplying the authorities with information unrelated to the offence in question. The warrant (…) was not sufficiently narrow in scope to prevent possible abuse" (§58-61).

Any act taken in the course of a judicial inquiry may be attacked in the first instance before the pre-trial chamber of the competent District Court, pursuant to Article 126 of the CPP. The seizure of digital (if not mobile) devices and/or of data has thus been examined in several sets of proceedings before the pre-trial chambers of the District Court of Luxembourg and of the Court of Appeal. In 2014, the pre-trial chamber of the Court of Appeal rejected a request by two companies to have searches and seizures carried out on their premises annulled, alleging that the judicial order was drafted too broadly (the appellants complained of a "fishing expedition"), insufficiently targeted on the offences in respect of which the investigating judge had been seized (which included direct taxation offences), and "betrayed" partiality on the part of the investigating judge. Whilst the latter two claims were rejected summarily, it is the reasoning used by the chamber in rejecting the first complaint which interests us here. Parts of the wording used in the warrant (e.g. "everything concerning…"; "everything which permits….") were indeed excessively (and regrettably) broad, agreed the chamber, but they were superfluous as other operative wording met the required levels of precision ("to identify the natural persons"; "to identify the legal entities"). More importantly:

> "The circumstance that the copies of electronic devices may contain documents with no connection to the targeted offences is without incidence on the validity of the operations at this stage of the seizure. It is now about proceeding to a sorting (*tri*) of the IT data copied onto external hard disks from the computers and USB flash drives of the companies and their administrators, issuing a *procès-verbal* of the seizure including an inventory of the relevant documents, and definitively erasing the documents which are irrelevant (*étrangers*) to the open criminal proceedings. The pre-trial chamber of the Court of Appeal notes that the appellants did not contest the validity of the judicial police investigators' mode of operation." (Ch. c. C., 24 November 2014, n°860/14)

The pre-trial chamber of the Court of Appeal thus validated what is reported to be the standard operating procedure for seizing data in three steps: making a "working copy" (agents of the SNT),

sorting and filtering relevant data (SNT), and issuing a new seizure order of the relevant data (investigating judge) (Kraus, 2017, p. 236). Writing in a personal capacity, an investigating judge (Martine KRAUS) has accordingly recommended documenting in the *procès-verbal* ('PV', a report) all steps of making a forensic copy of a server/hard disks, since the seizure of a copy of all data of e.g. a company is more susceptible to give rise to later challenges than a direct extraction of the relevant data (p. 231). It is however difficult to discern how often in practice a working copy of all data is taken, as opposed to performing filter and extraction on the seizure site. At interview, a member of the SNT remarked that in some cases where data extraction is performed at the place of seizure, time constraints and the terms of the judicial order may lead to potentially valuable data being left behind. This tends to occur where it is necessary to identify which part of data held by a third party company corresponds to the suspect(s), who may use aliases, etc., and it is not feasible to repeatedly revise terms of the judicial order. In relation to cybercrime, Putz writes that in practice "seizures are generally very broad and cover the entirety of IT equipment. For example, in child pornography cases, if files are found on one device, all devices and equipment found at the suspect's residence are usually seized and consulted. Holiday photographs and private messages are thus in effect copied onto the servers of the police. When drug dealers are arrested, the seizure of all mobile telephones is systematically made. For cybercriminals, the approach is the same" (Putz, 2019, p. 253).

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

Where technical tools are used to bypass security in order to access data seized from a mobile device, it would seem that in all cases the mobile device is also seized. As such, this question will be answered below in the section on "mobile device seized".

The question may also be taken to refer to the remote use of technical tools to bypass security on mobile devices. As stated in the answer to Q4, so-called digital searches (*perquisitions informatiques)* or less flatteringly "police hacking" is not at all covered in the Luxembourg legal framework and is thus very likely to be procedurally illegal and potentially constitute a criminal offence in itself.

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

As stated in several answers, data can be copied from any device in the course of a search; this is technically a seizure of data (Arts 33 & 66 CPP). When large volumes of data are seized (given that the visualisation of each file would be painstaking) investigators most often index all available

data, before searching within all data using keywords. Upon completion of the search by keywords, the relevant files and data are saved on a police device which the investigating judge may then seize in turn (Kraus, 2017, p. 236).

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

In accordance with the division between investigation (*enquête*) and judicial inquiry (*instruction)*, the *parquet* (translatable as "Prosecutor's Office") may, so long as an *information judiciaire* (a judicial inquiry) has not been opened, execute *inter alia,* searches, visits and seizures of *pieces à conviction* with the express – and, in principle, written – consent of the person involved (art. 47(1)-(2) CPP). Otherwise, as with any coercive measure, an order from an investigating judge will be required. Note that in any case a judicial inquiry is mandatory for *crimes.*

A limited exception to the *enquête/instruction* division is in place since 2010. Similarly to the Belgian reform which inspired it, the public prosecutor has been empowered to request that the investigating judge order a search of private premises, the hearing of a witness or an "expertise" without opening a judicial inquiry (*instruction préparatoire*), in relation to all felonies (*délits*) as well as certain specified crimes: use of forged documents, and theft with aggravating circumstances or with violence. Orders to "track and localise" telecommunications are also available in a *mini-instruction,* so long as the *délit* carries a correctional penalty of at least a year's imprisonment (art. 24-1(1), CPP).

In practice, there seem to be cases where consent is given by suspects to either copy data (e.g. from a social media account or email account) or to access open connections "in the cloud" discovered during a search; if consent is not given by the suspect, an order from the investigating judge is sought before a copy is made (GENVAL, 5.2.2., Kraus, 2017, p. 234).

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

The investigating judge may order any person – except the person who is the subject of the judicial inquiry, who retains the right to remain silent – to assist in giving access to seized systems or to data therein or accessible therefrom, as well as in understanding the protected or encrypted data (art. 66(4), CCP). This assistance is mandatory, but unlike in Belgium and France no criminal penalty is foreseen for those who do not comply with the judicial order.

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

Since in Luxembourg there is no remote "digital search" permitted by law, the person in **possession** of the mobile device will always be aware that it is being either seized (next section) or data is being extracted from it without seizure of the device – although this is unlikely for mobile devices.

The legal framework does not refer to the owner of the mobile device. In the judicial inquiry context, the officer of the judicial police draws up a report, or the investigating judge will make a PV, translatable as official report or statement, of his operations (art. 63(4) & 65 CPP). Seized data are inventoried in the PV (art. 66(2) CPP) which must be signed by the (suspect) *inculpé*, by "the person at whose residence the search and seizure have been executed" **and** by all present (article 66(5) CPP). If the *inculpé* refuses to sign, this is noted in the PV. A copy of the PV is left with the *inculpé*. There are no further legal requirements for the contents of a PV, and a standard paper form is used for all types of searches and seizures (*protocole de perquisition et de saisie)* with no distinction made for mobile devices / digital investigations.

In the event that the owner of the mobile device is not present, there is no rule providing that they must be informed. However, although the seized objects/documents/data are subject to the general secrecy of the judicial inquiry, there is nothing in the legal framework obliging third parties to keep secret the fact that a seizure has been carried out at their residence – that third party can inform the suspect/target.

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

This question seems to overlap to a great extent with Q5. Please see answer above.

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

It is difficult to answer such a broad question. It certainly matters very much whether "this person" (I presume the owner/person in possession of the mobile device) is the accused or not, given the central importance of the presumption of innocence and many more procedural rights under the EU's Roadmap Directives as implemented in Luxembourg law. As stated in answering Q9, the accused cannot be compelled to unlock/decrypt. However, it is unclear in what "matters" to the question here. As set out in other answers, the position of the accused and witnesses/third parties varies according to whether it is an *enquête* or an *instruction* – not least because the investigating judge is impartial and independent, seeking the truth rather than necessarily guilt. Moreover, "accused" fits uneasily onto criminal procedure in Luxembourg, where the target of an investigation may (in sequence) be a suspect, an *inculpé,* a *prévenu,* and eventually either convicted (*condamné*) or acquitted. Each status matters, coming with specific rules and jurisprudence – but as far as I know, nothing of specific relevance to mobile devices.

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

If you wish to give me some specific scenarios or stages of the criminal investigation/trial process, I will gladly follow up on this point.

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.*

Where data is not open source or access is not provided consensually, which would be within the wording of the Budapest Convention, the question of access in Luxembourg to data "in the cloud" outwith national territory has not been settled (unlike in French or German law). It is reported however that where access to IT equipment is itself gained legally, the police can also seize all "distant data" reachable from that equipment (Putz, 2019, p. 249).

As stated above at Q8, in practice there seem to be cases where consent is given by suspects to either copy data (e.g. from a social media account or email account) or to access open connections "in the cloud" discovered during a search; if consent is not given by the suspect, an order from the investigating judge is sought before a copy is made (GENVAL, 5.2.2., Kraus, 2017, p. 234). The reason given by prosecutors in the course of the Council of Europe evaluations was that arts 33 & 66 CPP on seizure "make no distinction between data in Luxembourg or abroad – as such, all data accessible from Luxembourg can be seized in the form of a copy" (5.4.3.).

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

Reflecting the strong influence on Luxembourg's criminal justice system of the Napoleonic tradition of separating the functions of *poursuite, instruction* and *jugement*, unless otherwise stated a judicial inquiry is mandatory for *crimes*, whilst it is optional for felonies (*délits*) – which the public prosecutor handles (art. 49, CPP).

The investigating judge may perform, in conformity with the law, any *acte d'information* which she deems useful to discovering the truth. She gathers and verifies, with equal care, the facts and circumstances tending to inculpate or exculpate (*à charge ou à décharge*) the *inculpé* (art. 51, CPP) An investigating judge may not sit on proceedings before the pre-trial chamber in relation to cases which she has instructed (art. 125*bis*, CPP). Likewise, investigating judges are prohibited from taking part in the eventual trial (art. 27(2) CPP).

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

The unequivocal independence of the investigating judge can be contrasted with the qualified impartiality of the public prosecutor (art. 51 CPP), who must investigate for both sides but only according to a "rule of conduct" – not a procedural rule, making it very difficult to base claims for nullities thereupon.

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.*

Please see answers below with regard to inadmissibility of evidence.

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

Mobile device seized

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

Yes, according to the seizure provisions in the CPP (principally art. 66(1) in conjunction with art. 31). There is no limitation with regard to either device type or data type in these broadly-termed powers: searches may be carried out in any place where objects may be found which could be useful for the discovery of the truth (Art 65 CPP) and the investigating judge's powers of seizure are all-encompassing, covering *inter alia* any object, document, effects, data stored, processed or transmitted in an automated data processing or transmission system. The power also covers 'effects' which have been used to commit the crime or which were destined to be used as such and those which have formed the object of the crime, as well as everything which appears to have been the product of the crime, as well as in general, all that appears useful to the discovery of the truth or the use of which would be of such as nature as to harm the good workings of the judicial inquiry and all that is liable to confiscation or restitution (Art. 31(3) CPP).

In Luxembourg the seizure of digital evidence generally is to a large extent regulated identically to the gathering of any other form of evidence. A notable exception is found in the changes made to the CPP by the 2014 law implementing the Budapest Convention and codifying certain baseline procedural steps for the seizure of stored content data by the investigating judge (in the typical scenario of the judicial inquiry), the public prosecutor (in the very limited *mini-instruction* scenario) or the judicial police acting unsupervised (in urgent cases of *délit flagrant*). As detailed above, these adjustments include express provisions on the making of copies – rather than the seizure of physical electronic devices – and on the enlisting of decryption experts.

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

In practice, the judicial police typically executes seizures on behalf of the investigating judge, systematically involving members of its SNT. An exception is urgent cases (*délit flagrant*), where seizures of devices may take place according to the same rules set out above at Q5 for searches and for seizures of data. Otherwise, the broad rule in art. 66 CPP applies (see Q16).

Below the provisions of the CPP, no soft regulation or checklist of operations for digital seizures were uncovered by desk research or through an interview with two representatives of the SNT, and this observation is borne out in several decisions of the pre-trial chambers of the "instruction courts" detailed throughout this questionnaire. Writing in a personal capacity, an investigating judge has stressed the importance of taking precautions in order to ensure data on seized devices are not modified, warning that "although the SNT's specialised investigators know how to react

regarding seizure of computers or smartphones, this is not necessarily the case for all police officers who have to carry out searches in the course of their duties" (Kraus, 2017, p. 227). The judge advises that police officers follow *Electronic evidence – a basic guide for First Responders,* published in 2015 by ENISA, and insists that when examining a switched-on computer on the seizure site, "the investigator must absolutely document the different stages of their intervention".

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

Yes, unless the defence launches (within 5 days) a successful challenge to the seizure pursuant to Art. 48-2 CPP, and the mobile device has not yet been 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?*

*Question uses "search" but the section is on **seizures** of mobile devices.

In keeping with the investigating judge's independence, there are no limits to what she may examine having seized a mobile device. According to Putz (2019, p.236) when a mobile telephone is seized it is normal procedure to extract all data therein using special software (no name/brand is given) – all data then goes into the *dossier*. The same author shares a "particular" case of banking card fraud wherein one of the "girls" accused maintained before the investigating judge and the trial court that she had a serious project of opening an cupcake business online. Although having no bearing on guilt, this kind of circumstance can influence the eventual penalty. As all data from the mobile telephone was available in the dossier, the court was able to see hundreds of photos of pastries – to the benefit of the accused (TA Lux., 18e, 25 octobre 2018, no. 2707/2018).

One golden rule for searches as well as seizures is proportionality – which the pre-trial courts have often examined in relation to seizures of digital devices and data. In one notable case, the legality of judicial orders to seize data stored in Luxembourg was challenged in the course of a complex, tortuous affair entailing accusations of kidnapping and murder in Kazakhstan, letters rogatory issued in relation to spying and duress (*Nötigung)* in Austria, and finally allegations of criminal breaches of data protection legislation in Luxembourg. In relation to the latter, "domestic" proceedings, two judicial orders had been simultaneously executed on a company storing data in Luxembourg on behalf of an Austrian law firm.

One order was annulled on proportionality grounds, with the pre-trial chamber of the Court of Appeal eventually concluding, "in view of the enormous quantity of data stored on the seized devices" that the search and seizure constituted a search for as-yet-unknown offences, prohibited by the CPP (arts 31(3), 66 & 50). The order sought seizure of two HP servers, a hard disk, and over a hundred cassettes dating back to as early as 2001. It was annulled partly due to its covering data generated at a time when the criminal acts under *instruction* could not possibly have been committed, and annulled entirely due to its covering "the totality of the legal office's IT devices located in Luxembourg without a selection being made between the data relating to the affair (…) and the legal office's other documents unrelated to this affair".

The other order concerned not raw data to be seized in the field, but twelve hard disks in the possession of the SNT, containing the results of a *filtrage informatique* which had previously been carried out on data seized pursuant to earlier letters rogatory issued by Austria to Luxembourg. In fact, those initial proceedings had been closed in Luxembourg after the Austrian prosecutor's decision to issue letters rogatory was subsequently annulled by an Austrian court. Upon annulment in Austria, the Luxembourgish investigating judge ordered the release (*mainlevée*) and restitution of all seized data, before immediately seizing it again – this time in relation to fresh allegations made in the meantime in Luxembourg. The pre-trial chamber of the District Court of Luxembourg decided that this background posed no problem with regard to the first order, on the grounds that it targeted the same data which the investigating judge could hypothetically have seized in the absence of any Austrian request for mutual legal assistance. The second order, on the other hand, targeted data which "owe their existence" to and had been "confected" on the basis of an act of mutual legal assistance which had since been revoked. Adding that it was not convinced of the usefulness of the data to the discovery of the truth, the chamber annulled the order and recalled an earlier decision establishing that the destruction of IT data across all police systems is an automatic corollary of the restitution of objects which have been seized illegally (Ch. c. C., 18 June 2014, n° 423/14).

Whether seizures are carried out by the judicial police unassisted (in the urgent *crime flagrant* scenario) or under the supervision of the investigating judge, "all useful measures" must be taken in advance (*préalablement*) in order to ensure the respect of professional secrecy and of the rights of the defence (arts 33(3) & 65(4) CPP). Lawyers' workplaces and the confidentiality of their communications with clients are in principle inviolable (art. 35(3), Law of 10 August 1991 on the legal profession, Mémorial A No. 58). When any measure *inter alia* of a judicial inquiry is carried out "upon or regarding a lawyer" (*auprès ou à l'égard d'un avocat*), the president of the Bar (the *Bâtonnier*) or his representative must be present. The latter may address his observations concerning the safeguarding of professional secrecy. The seizure act and the search PV must mention, on pain of nullity, the presence of the *Bâtonnier* or his representative, as well as any observations made by the latter. Furthermore, jurisprudence has considered that the application of the rules of criminal procedure may be influenced by internal regulations (*règlement d'ordre*

intérieur) issued by the Bar Council (*Conseil de l'ordre du Barreau de Luxembourg*) (See Article 19, Law of August 1991 on the legal profession, cit., and Ch. c. C. n° 316/12, 23 May 2012).

All of these provisions received ample application in notorious proceedings before the pre-trial chambers in 2014, which concerned coordinated searches and seizures targeting lawyers and revealed a veritable litany of procedural errors (Ch. c. Lux. (*Chambre du conseil, Tribunal d'arrondissement de et à Luxembourg*), 2 April 2014, N° 927/14). The sheer disproportionality of the seizure of devices/data executed is extraordinary: whereas just one lawyer was suspected of criminal wrongdoing, seizure was made of all of the electronic files of the legal office – where at least six lawyers worked!

In an admonitory tone, the pre-trial chamber of the District Court of Luxembourg recalled that "the seizure of electronic files cannot accord more freedoms to the seizing authority than physical documents", and remarked that the latter evidence had by contrast been seized in application of precise search criteria. Making direct reference to the emphasis placed by the European Court of Human Rights in *Wieser v. Austria* on the strict observance of procedural rules requiring the compilation of a report at the end of a search along with a list of seized objects, the chamber strongly condemned the PVs of both the investigating judge and the police for not detailing "concretely" how the provisions of Article 66(2) CPP had been respected in light of the reservations expressed by the lawyers during those operations. Again citing analogous reasoning from *Wieser,* the chamber also criticised the execution of multiple acts of search and seizure in several different locations on the same day; in the chamber's words, the representative of the *Bâtonnier* could not "be present everywhere at the same time". In sum, the chamber found nothing in the dossier submitted to it showing fulfilment of the injunction in Article 33(3) CPP to "take (*provoquer*) in advance all useful measures" in order to ensure respect of professional secrecy and of defence rights. Annulment, restitution and destruction of all seized data across police and judicial systems were duly ordered.

Shortly thereafter, in another decision revolving around the seizure of data from a law firm, the pre-trial chamber of the Court of Appeal approved just such "useful measures" (Ch. c. C., 11 November 2014, N° 824/14). In this case, all parties (the lawyer suspected of criminal wrongdoing, his lawyer, the investigating judge, the *Bâtonnier* and the SNT police officers) agreed in advance in writing that the hard disks from the law firm's computers would first by copied (at the law firm) onto police hard disk drives, and that the latter would be placed in a sealed room (*mis sous scellés*) within the offices of the police. The police would only be able to enter this room in the presence of the *Bâtonnier* (or a representative) and a representative of the law firm in order to proceed, using special software, to the indexation of the copied data and their exploitation by keyword. Should results emerge from the analysis, the documents found would be listed in a PV along with any observations the *Bâtonnier* may wish to make in respect of their relevance to the aims of the judicial inquiry. In this case, the results were first handed to the lawyers under investigation in order for them to verify which data the investigators considered "useful to the discovery of the truth". A meeting was subsequently called at which the lawyers, their counsel, the *Bâtonnier* and a magistrate

from the public prosecutor's office were invited to comment on the seizure of those data. The investigating judge then decided which data to seize.

The chamber deemed this procedure to allow maximum preservation of the interests and rights of the parties involved: once the data had been copied the firm could continue using its computers as per usual, the sealed room solution excluded "any clandestine manipulation of the copied data", and the definitive erasure of the irrelevant data – which could be verified by the parties – made it impossible to carry out investigations into activities which were not targeted by the judicial inquiry. The potential of such methods, however, remains open to question (at least) on resources grounds. Writing in a personal capacity, a leading investigating judge has thus remarked that in the case at hand, the judicial police had to dedicate an office exclusively to the analysis for several months, with its duration unsurprisingly stretched by the need to assemble all representatives for each entry and session. As such, parsimonious use of such measures by the investigating judge is not only advised but inevitable (Kraus, 2017, p. 233).

Follow-up proceedings in the "useful measures" case described above – concerning seizures carried out at law firm's offices – have led the pre-trial chambers to address two further technical aspects of the proportionality of the "copy, filter, share, seize" process, applied in that case to lawyer-suspects (Ch. c. C., 8 July 2015, n° 596/15).

On the one hand, the defence argued that the copy made at the law firm had not been sufficiently limited temporally in order to target as precisely as possible the documentation relating to the lawyer-suspect. On this point, the pre-trial chamber of the Court of Appeal decided in favour of the investigators: as it had not been demonstrated that the dates of files and folders could not have been manipulated or hidden, a search based on visible dates would risk failure.

On the other hand, having received the results of the police-operated filter the defence complained of differences between the keywords featuring on a list shared with them (pre-filter) and those used in reality by police analysts – leading to an overly-broad analysis akin to a "fishing expedition" and hampering the effective use of the defence of the shared results (since the keywords involved at different stages are either not included or are redacted in the text of the decision, it is not possible for the reader to gauge precisely the entire procedure). The pre-trial chamber of the District Court considered that the defence had had ample opportunity to challenge the use of keywords, either by addressing their observations upon learning which keywords would be applied to the data (which they had in fact done, by email) or by challenging the seizure of data effected using contested keywords, or at least to have observations in that regard taken down, upon formalisation of the seizure (Ch. c. Lux., 8 May 2015, N° 1297/15).

The pre-trial chamber of the District Court declined, however, to specifically address whether the use of "new" keywords could have any impact on the integrity (*régularité*) of the procedure. This issue thus fell to the pre-trial chamber of the Court of Appeal, which referred back to the very role of the investigating judge, who proceeds to all acts of *information* which she judges useful to the discovery of the truth, and thus stated the chamber is "free to use the keywords she judges the most appropriate to the search for relevant documents without being blamed for (*sans qu'il puisse lui*

être reproché) the discrepancy between the relatively small volume of documents with a link to the facts in relation to which she is seized and the scale of the documentation that she is called upon to verify during her inquiry".

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

Similarly to the answer to Q8, without the consent of the owner/person in possession of the mobile device, the public prosecutor will not (where he is competent) be able to force seizure: a judicial order from an investigating judge will be required. An exception is the scenario of *flagrant délit,* as detailed in several places above.

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

The investigating judge may order any person – except the person who is the subject of the judicial inquiry, who retains the right to remain silent – to assist in giving access to seized systems or to data therein or accessible therefrom, as well as in understanding the protected or encrypted data (art. 66(4), CCP). This assistance is mandatory, but unlike in Belgium and France no criminal penalty is foreseen for those who do not comply with the judicial order.

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

Please see answer to Q10 above.

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

Yes, and it is reportedly not unusual for access or decryption to be handled by private third parties in other (European) jurisdictions. In the cybercrime context, it was reported in 2017 that the SNT had in the past used specialists from CIRCL (Computer Incident Response Center) Luxembourg, from Europol-EC3 or automated tools from private enterprises for the examination of malware (GENVAL, 5.2.2). There is no digital forensic laboratory in Luxembourg other than that within the

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

SNT, composed of IT forensic experts who double as police officers, and who carry out all relevant analysis "in-house".

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

An unclear question ("does it matter" could be interpreted in endless ways); please see answer to Q12.

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.*

Please see answer to Q13 above.

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

Please see answer to Q13 above, which also refers to "loss of location" situations.

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

Please see answer to Q13 above; although the legal situation is blurry, it is reported that in practice an "open connection" is considered exploitable by investigators, and that all data that can be accessed from a mobile device is "fair game". I am unsure whether this is distinct from "app that links to this data or other direct link from the mobile device", as the question puts it. Nothing in

the legal framework would appear to block investigators from connecting to apps/services/websites on the mobile device, for example using usernames, passwords or access codes recovered from the search site (e.g. on physical documents, post-its, diaries etc.; Putz, 2019, p.247) and, for instance, web search history.

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?*

In general, basic subscriber information is supplied voluntarily, whilst any other type of data (especially content) requires a judicial order from an investigating judge. For more detail please see answer to Q36 below.

This is a very broad question ("data… related to the device"). There is a mix of voluntary and mandatory cooperation between service providers and law enforcement / judicial authorities, but it depends very much on the type of service provider and the data type (subscriber and usage data / traffic and location data / content data). I can provide more details, if relevant.

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

Please see answer to Q14.

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 see answers in Section 3 below: Admissibility.

Please, answer all these questions separately for each scenario or instance which, in your opinion, is (partially) subject to different rules than other scenarios. At least, make the difference between the scenarios where a mobile device is seized and where it is not. If all sub-scenarios in one of

these scenarios are the same, it suffices to only answer the questions once. However, most jurisdictions have different situations in which seizure is possible (e.g. in the context of a search of premises vs. not in the context of a search), so please differentiate between these scenarios, as well and answer the questions for them separately. If you prefer, you can answer the questions in their totality in an integrated explanation, as long as all elements are covered and again, various scenarios are differentiated between.

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

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

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

I am unsure of what "changing configuration" might cover; please see answer to Q37 below.

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

There are no such rules.

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?*

Art. 7-2 CPP establishes that "any offence of which an act characterising one of its constitutive elements has been committed in the Grand Duchy of Luxembourg shall be considered to have been committed on the territory of the Grand Duchy". Jurisprudence has expanded on this construction,

holding that "the element to be taken into consideration as the localisation criterion is the material element, whether the delictual conduct or the result produced by the act" (*Cour de cassation,* N° 14/2014 *pénal*, 13th March 2014, p. 2), and that the act characterising one of an offence's constitutive elements must have taken place "entirely" on Luxembourgish territory in order to trigger jurisdiction (*Cour d'appel,* 11th March 2008). In general, where the damage has occurred in Luxembourg, this will suffice; merely preparatory acts, on the other hand, will not reach the threshold (GENVAL, p. 55). There also exist many provisions in the CPP providing for extraterritorial jurisdiction where the offence is committed abroad but the perpetrator is either a Luxembourg national or resident or a foreign citizen present on Luxembourg territory (see arts 5 – 7-4 CPP). In practice, I was informed that the location of data sought is detected using WHOIS; where this method is not available, the location of the headquarters of the company is generally used as the location of the data (Police). Other contacts mentioned IP address as the sole criterion (Ministry) and confirmed that the police investigation will determine where the data are stored (Prosecutor).

In cases of parallel investigations between multiple states, it is the *parquet général* which deliberates whether to renounce investigations, taking various factors into account including the nationality and location of the suspect, nationality of the victim, level of harm/damage, the status and progress of the investigation, and respect of defence rights (GENVAL, p. 59). Luxembourg did not implement Framework Decision 2009/948/JHA of 30 November 2009 on prevention and settlement of conflicts of exercise of jurisdiction in criminal proceedings, but is an active member of Eurojust. At least in the cybercrime context, no significant concerns regarding conflicts of jurisdiction are reported: the states generally reach an agreement via their respective central authorities (on the Luxembourg side, again the *parquet general*; GENVAL, p. 57).

The nature of direct cross-border cooperation between judicial authorities by design strips away one level of procedure in the form of centralised control of outgoing MLA requests or EIOs. The *parquet* or *juge d'instruction* is thus empowered by such arrangements to make requests directly to counterparts, according to the terms of the base agreement. Should there be no such set-up or, alternatively, no bilateral international convention in place with a country, Luxembourg law still provides no general legal framework for outgoing MLA requests, which "is more a question of good sense than law" (Lugentz et al list as principal factors in any decision to request MLA (1) the usefulness of the act requested, (2) the proportionality of the means envisaged, (3) the probability of obtaining a result and (4) in keeping with Article 6 ECHR, the length of time likely required in order to obtain the solicited material – especially in cases of preventive detention; pp. 754 *et seq*).

Nonetheless, by virtue of its being an act of investigation or of *instruction*, the decision taken in Luxembourg by either the public prosecutor or an investigating judge to issue letters rogatory or an MLA request to colleagues abroad is open to challenge before the pre-trial chamber of the district court according to the provisions of the CPP (art. 48-2). However, since the concrete

investigative measures thereby requested by the judicial actors in Luxembourg are eventually executed in the other jurisdiction involved (thereby escaping national judicial control), litigation concerning the initial request is reported to be rare (in contrast – historically – to challenges to incoming MLA requests – where investigative measures are executed in Luxembourg). There is no recourse to the pre-trial chambers foreseen for EIOs issued by Luxembourg in the recent implementing law.

For incoming MLA requests, the standard *'loi de 2000'* (law of 2000) (*Loi du 8 août 2000 sur l'entraide judiciaire internationale en matière pénale*) remains applicable, but residually, i.e. if the provisions of any tailored agreement are different (e.g. bilateral MLAT), the latter provisions take precedence.

***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?*

Within the EU Area of Freedom, Security and Justice, on 15th September 2018 the EIO implementation law replaced the *loi de 2000* along with all of the main multilateral MLA Conventions and Treaties (1959 MLA Convention, CISA 1990 and the 2000 MLA Convention (as stipulated in Article 34 of the EIO Directive) plus the 1962 Benelux Treaty as concerns relations between Luxembourg and other EU Member States having also implemented the EIO Directive (arts 34 & 42(1), EIO implementing law). Moreover, the new law also stipulates that requests for assistance originating from "States" which have not implemented the EIO Directive – meaning, presumably, EU Member States – shall be "assimilated" to requests made on the basis of the provisions of the EIO Directive and examined in accordance with the provisions of the implementing law (Art.42(2).

Notably, the EIO implementation carries over several provisions from the *loi de 2000*, devoting a separate section (Ch. 3 s.2) to the procedure applicable to EIOs issued by another Member State to Luxembourg in the aim of having *coercive* measures executed. In particular, all EIOs requesting a seizure of objects, documents, funds or assets of any nature, the communication of information or documents, a search or any other act of *instruction* presenting an analogous degree of coercion must be addressed to or – where an EIO is sent directly to a judicial authority or the justice minister – forwarded to the *procureur général d'État* for a centralised examination (arts 21-22).

***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?*

It is unclear whether the question refers only to relations between EU Member States (please see answer to Q34; EIO takes precedence) or also with third countries. In the latter case, as stated above there is no general legal framework for outgoing MLA requests, whilst incoming MLA requests are subject to the residual '*loi de 2000*'. In case it is useful, I will provide some background information on MLA requests issued by Luxembourg, and then MLA provided by Luxembourg to foreign authorities – all in relation to electronic data, with no limitation to data related to mobile devices.

Without specifying countries with which Luxembourg cooperates in practice, one contact stressed that due to the small size of the country "evidence … can be found in our neighbouring countries or even on a wider level" which may be pertinent to "nearly every bigger criminal case in Luxembourg" (Police). It is in many cases very difficult to obtain electronic data from certain (unnamed) third countries (Judge). Although no official statistics exist, one contact cited organised crime, cybercrime and financial crime as the most important offences (Police) – supported by a view from academia which mentioned child pornography, financial crime and hacking (Academic).

Although no official statistics exist, according to one contact it takes on average 120 days to receive electronic data requested from an EU Member State, and up to 300 days where it is requested from a third state (for example the US) (Ministry). Where data are stored in another country, underlined a prosecutor, international requests for cross-border access take longer since they depend on the workload and willingness to assist of the receiving judicial authority (Prosecutor). One contact cited verification of the validity and legality of requests, the volume of data requested, and encryption of data as the main challenges in this regard (Ministry). Another emphasised that "the knowledge of what information is available where and how might take time to acquire"; thereafter, letters rogatory must be drafted – but "most of the time" is taken up by waiting for a reply (Police). According to one contact from the legal profession, the slow handling of requests emitted by Luxembourg can be ascribed to the lack of willingness of receiving authorities, along with a lack of dynamism on the part of the Luxembourg authorities, who are not very "aggressive" in chasing up requests (Lawyer).

Turning to cooperation given by Luxembourg, before the existence of the EIO the most frequently-used ground invoked in order to refuse a request for judicial cooperation of all kinds was that the request was not formulated in accordance with the requirements of the *loi de 2000*. My understanding is, however, that in the case of seizure of electronic data, Luxembourgish refusals to cooperate are "very rare" (Prosecutor). Another contact observed that in general, investigating judges in Luxembourg are able to obtain requested data from service providers operating in the country, especially where more serious offences (terrorism; child pornography) are being investigated (Judge). With regard to electronic data, one contact (from the central authority which receives all requests for cooperation sent to the Luxembourgish authorities) remarked that requests

may in practice come from judicial authorities of EU and non-EU states, or from international judicial authorities recognised by the Grand-Duchy of Luxembourg (Prosecutor). One contact noted that the European headquarters of several large technology-related companies (Skype, Amazon and Viber) are located in Luxembourg (Police), but the extent of cooperation on electronic data remains unclear. Indeed, compiled statistics on all letters rogatory received by the authorities in Luxembourg are published annually (available at https://justice.public.lu/fr/publications.html (in French)). A separate subsection is devoted to statistics on "e-commerce letters rogatory", covering eBay, Amazon, PayPal, Skype, iTunes, Blockchain (sic), Bitstamp, Viber, and Six Payment, which oscillate between a quarter and a third of all letters rogatory received. Amazon declined to speak on the record, but one contact mentioned that Luxembourg regularly receives requests from the US and from Russia concerning Skype data (Judge). Two contacts underlined that although several of the major service providers have European headquarters in Luxembourg, their data are stored elsewhere (Police; Judge). Depending on the company and the specific circumstances of the request, accessing electronic data may require a further request to the responsible department further afield (Judge), or international headquarters may provide the data to European headquarters in Luxembourg (Police), meaning that a domestic judicial order suffices. It would appear, therefore, that cooperation currently works on a case-by-case and client-by-client basis.

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

"Cooperation mechanisms and practices" is potentially quite broad – one could think of the training of civilian IT experts as police officers for the SNT, cybersecurity initiatives helping aiming to improve the security of passwords, etc. – perhaps to be developed at interview.

In terms of obtaining or supplying electronic data in cross-border cases, this has been partly answered in Q35.

Domestically, Luxembourg sits near the top of several regional and international indexes for ICT development, digital economy and society, and technological readiness (L. Funck (2019), 'Luxembourg' in J. P. Lanka (ed.), *The Technology, Media and Telecommunications Review* (9th edition, January 2019), 235.) and hosts an impressive and growing number of data centres along with the regional or global headquarters of major internet and e-commerce players including Skype, Amazon and PayPal (all European HQ) and Viber (global HQ). Although targeted official statistics are not compiled, my research indicates that Luxembourg's small size, highly-connected nature and financial strength translate into active cooperation between service providers in criminal investigations in both domestic and cross-border situations. Depending on the type of service provider, type of data sought, and applicable legal basis, such cooperation may be voluntary, *de*

facto mandatory as a corollary of being regulated, or *de iure* mandatory – but with the emphasis firmly on the latter scenario, i.e. via binding duties set out in the CPP.

Existing reports and research have suggested that cooperation within Luxembourg between judicial authorities and Internet and other service providers works fairly smoothly in practice – although the remit of the few (and now somewhat dated) available studies is limited to particularly grave offences: child sexual abuse online and the use of the internet for terrorist purposes (*Global Alliance against Child Sexual Abuse Online – 2014 Reporting Form of Luxembourg,* at 2. Available at https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/global-alliance-against-child-abuse/docs/reports-2014/ga_report_2014_-_luxembourg_en.pdf) and CODEXTER Report on the use of the internet for terrorist purposes in Luxembourg, October 2007). More recently, regarding cybercrime a Council of Europe evaluation on Luxembourg's capacities in that domain also found that local branches of private companies cooperate voluntarily with regard to BSI (basic subscriber information), and that overall cooperation is very good. More generally, see the first listed recommendation (of seven) made by GENVAL in 2017 to the European Union, EU institutions and other Member States: "The Member States should take inspiration from the good practice identified in Luxembourg by the evaluation team, including the very good collaboration between public and private sectors" (GENVAL, 9.2.2).

Companies do not, on the other hand, transmit information that *they* adjudge to have no link to Luxembourg – and this decision is unregulated and usually not transparent. In such cases, in order to access BSI – as well as for instance content data – the police must ask an investigating judge to issue letters rogatory, considerably slowing down the process. This picture is reinforced by an interview with a specialised public prosecutor carried out at the University of Luxembourg in the context of a research project which revealed (in 2014) that: "cooperation with service providers other than providers hosting information provided by a recipient of the service (such as Facebook) is quite good in practice, especially if those providers have their headquarters, an office or at least a contact point in Luxembourg. By contrast, the cooperation with service providers located abroad is reported to be far from smooth; those providers usually only hand over basic subscriber information" (Franssen & Ligeti (2014), p.20).

In the same vein, although revealing statistics are still scarce, for instance of 470 "cyber" dossiers recorded in Luxembourg in 2015 a large majority (370) were classified as having been committed by an unknown person – although damage levels were very high. The causes mentioned by the national authorities were: impossibility of identifying perpetrators, the international nature of the type of offences and difficulties in cooperation and mutual legal assistance matters. Another obstacle was the fact that "ISPs" do not cooperate and the data are not located in Luxembourg (GENVAL, 2017). It is conceivable that to some degree the presence of the European headquarters of major service providers in the Grand Duchy means that law enforcement is obliged to focus on those investigations which can draw on whatever data is accessible locally. Notably, one view from

practice suggests that this is quite often the case, even regarding foreign ISPs without an office in Luxembourg, because they usually keep a copy of their data mirrored on local servers, obviating the need to resort to mutual legal assistance ('MLA') (Braun, 2014, p.132).

Lastly, from an operational perspective, in 2017 the "New Technologies" section of Luxembourg's Grand-Ducal Police was cited – in the cybercrime context – as an example to the rest of Europe with regard to its composition, its tasks and its positioning at the international level. In particular, the possibility for "civilian" IT experts (from the private sector) to qualify as officers of the judicial police was adjudged to enable a fruitful *rapprochement* of skills, which Council of Europe evaluators put forward for development at the European level (GENVAL, p. 32).

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.

The rights of the defence, although absent from the Luxembourg Constitution, were attached to Article 12 thereof ("No-one may be *poursuivi* – pursued/prosecuted — other than in cases foreseen by the law and in the form prescribed by the law") by the Constitutional Court in a 2013 judgment (C. const., 25 October 2013, decision n° 104/13). Furthermore, since Luxembourg follows the monist tradition regarding the status of international treaties in domestic law Luxembourg judges give direct effect to individual rights featured in the ECHR as well as to EU Directives, which prevail over national legal provisions. Key examples of European influence on Luxembourg domestic law in the digital investigations context are the right to access to a lawyer, and the request

to annul evidence which has been illegally or improperly obtained which may be founded – according to jurisprudence tracing back to 2012 – on alleged violations of the right to a fair trial guaranteed by Article 6 ECHR (CSJ Ch.c.C. 16 May 2012, n° 301/12; CSJ Ch.c.C. 22 October 2012, n° 674/12).

Insofar as mobile forensics involve personal data, the processing of such data is subject to the provisions of the LED, as implemented in Luxembourg in 2018 (Law of 1st August 2018, Mémorial A Nº 689, 16 August 2018). The new domestic rules apply broadly to the "processing" – implemented identically broadly as in the LED – of personal data by the police and judicial authorities in the course of their core functions: the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties. Several principles, obligations and data subject rights found in the LED implementation are of direct or indirect relevance to mobile forensics – for example, duties to keep a register of processing activities, along with rules on data security, retention periods, and informing data subjects of the processing of their data. Very little information is available as yet on how fulfilment of these duties is actually handled in practice. The compliance of police and judicial actors with the implementing law will be monitored by both the national data protection authority (the *Commission nationale pour la protection des données,* 'CNPD') and a newly-created, specialised *Autorité de contrôle judiciaire* (Ch. 6, LED implementation law).

Article 23 of that law imposes a horizontal duty on data controllers to keep a register of all categories of processing activities under their responsibility including *inter alia* the name and contact details of the controller, the purposes of the processing, an indication of the legal basis for the processing operation, and descriptions of the categories of data subject and of the categories of personal data. Data processors (*sous-traitants)* are also subject to less stringent record-keeping requirements. Automated processing systems are subject to specific logging (*journalisation)* requirements in Art. 24 of the implementation law, in the aim of making it possible to establish the justification, date and time of such operations and, as far as possible, the identification of the person who consulted or disclosed personal data, and the identity of the recipients of such personal data. The logs shall be used solely for verification of the lawfulness of processing, self-monitoring, ensuring the integrity and security of the personal data, and for criminal proceedings (Art. 24(2), LED implementation law).

Other than that, there is no specific legal duty to write a report on mobile forensics operations. Nonetheless, according to our interview with the SNT, records of processing are systematically kept. This is supported by comments from an investigating judge, who writes that in each dossier in which it is involved, the SNT summarises the results of its research in a report which goes into the criminal case file and is thus available to the investigators, the investigating judge, the defence, the public prosecutor, the pre-trial chambers and the trial courts (Kraus, 2017, p. 236). As stated, there are no rules on how such a report must be compiled, but again according to the SNT interview it is a fairly regular occurrence for judges to question police officers in the pre-trial chamber on the

methods they have used in their analysis. Using the same forensic analysis method as is used abroad "by the majority of experts", writes the judge, ensures that an outside expert may also examine the original seized physical device without its content having been modified by the SNT's analysis – by extension, this ought to protect too against discrimination. It has also been reported that in practice copies are often made using a dump, allowing for preservation of the state of data at a certain moment in time; hash value calculation will thereafter reveal any subsequent alteration (Putz, 2019, p. 264).

Seized data are deposited at the registry (*greffe*) of the competent District Court or with a *gardien de saisie*, pending resolution of the proceedings (Articles 33(7) & 66(6) CPP). There appears to be no limit on how long seized data may be stored at the *greffe*, should no nullity or action for restitution be founded. As noted above, where a nullity is granted by the pre-trial chambers of the instruction courts, the destruction of all data is automatically ordered across all police systems. Otherwise, according to Articles 4 and 7 of the LED implementation law, retention periods for personal data are set by the data controller in light of the goal of the processing, procedural rules must be in place to that end, and those rules must be communicated to data subjects. At interview, members of the SNT stated that a project is currently underway in order to improve the "follow-up *informatique"* i.e. who performed which part of the chain of custody, and where precisely specific evidence is stored.

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?*

There are no specific conditions or constraints in Luxembourg law regarding the admissibility of electronic evidence in criminal proceedings (confirmed in GENVAL, p. 51). Furthermore, the fundamental principle of free assessment of evidence by the Luxembourgish trial judge (*la liberté de la preuve*) means that any type of evidence is *a priori* admissible before the criminal courts (see e.g. V. Bolard, *Preuve et vérité* (trad. "Evidence and truth"), in *Annales du droit luxembourgeois,* Vol. 23, Bruylant, Brussels, 2013, p. 39, p. 75).

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

Yes, the criteria are the same, but the situation plays out differently depending on whether it is an *enquête,* an *instruction,* or lower-level proceedings. I will elaborate on the central concept of the

legality of evidence. In the judicial inquiry context illegally or improperly obtained evidence can be excluded by the pre-trial chambers (of the "instruction courts") on the basis of Article 126 of the CPP. In the preliminary investigation (*enquête*) scenario, since there is no judicial inquiry stage, the admissibility of evidence is resolved before the eventual trial court – but before any review on the merits, pursuant to Art. 48-2(3) of the CPP. The goal of the legislator is clearly to have all admissibility issues adjudicated as early as possible – and ideally before trial. To that end, should an *inculpé* fail to trigger a nullity before the pre-trial chamber or should the chamber reject such a request, the trial court has no power to apply nullities during the proceedings referred to it (*purge des nullités*). Nullities which can be engaged before the pre-trial chambers may be formal (foreseen in a statutory provision) or substantive (developed in jurisprudence in order to sanction violations of substantive procedural requirements – in particular, breaches of defence rights). Since 2012, the jurisprudence considers that a request for nullity can be based on alleged violations of the right to a fair trial enshrined in Article 6 of the ECHR (Ch. c. C., 16 May 2012, n° 301/12).

A fortiori given its monist tradition the presumption of innocence, enshrined in Article 6(2) and developed through Strasbourg jurisprudence emphasising the burden of proof resting on the accusation, is of central importance to the criminal justice process in Luxembourg (See e.g. Cass., 28 April 2016, n° 17/2016, p. 25). The right to be heard and to give evidence is inherent to the adversarial nature of hearings at the trial stage for felonies and crimes, with a raft of protections set into the CPP and in case law, such as the right of reply *(droit de réplique)*, in effect the right to speak last in order to effectively challenge arguments put forward by the public prosecutor (arts 190-1(3) & 222, CPP).

In the context of misdemeanours (*contraventions)*, which are judged by either the lower-level police courts or the correctional chambers of the district courts, reports by judicial police officers are presumed true until it is proven that the officer falsified the report (arts 154 & 189 CPP). No such rule applies, however, where felonies (*délits*) are adjudicated by the correctional chambers of the district courts, or where crimes are adjudicated by the criminal chambers of the district courts. Furthermore, there are no specific rules concerning the chain of evidence. At interview, members of the SNT remarked that in practice judges often ask how certain results were obtained or conclusions were reached in the course of digital investigations. Although it was unclear in what degree this remark referred to the pre-trial or the trial stage, for that reason where possible the SNT use open source software, so that steps taken may be explained to the judge(s) in detail, and potentially contested by the defence.

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?*

In 2007, a landmark judgment of the *Cour de Cassation* established the rule that the trial courts may discard evidence that has been unlawfully obtained if either (i) the non-respect of certain formal requirements is sanctioned by nullity; (ii) the irregularity committed has tainted the credibility of the evidence; or (iii) use of the evidence is contrary to the defendant's right to a fair trial.[2] It is "nonetheless" for the judge to evaluate the admissibility of illegally-obtained evidence taking into account the elements of the case considered as a whole, including the manner in which evidence has been obtained and the circumstances of the illegality committed – in other words, even if none of these three alternative criteria is satisfied, evidence may still be discarded should the *légalité* of the administration of evidence not be ensured overall. In this connection, the Court of Appeal has held that the adversarial discussion of evidence at trial does not suffice to repair irregularities in the gathering of evidence (Cass. 22 November 2007, n° 57/2007 and C.A. 26 February 2008, n° 106/08). The Court's position in favour of the inadmissibility of illegally-obtained evidence is stronger than that of its counterparts in Belgium and in France (M. Marty, *La légalité de la preuve dans l'espace pénal européen*, Larcier, Brussels, 2016, p. 274-313).

In a 2015 ruling, the pre-trial chamber of the District Court of Luxembourg explicitly recognised that due to the absence of any specific legal provisions in Luxembourg governing seizures of computer data, the instruction courts are to evaluate the conformity of each challenged seizure, case-by-case, with regard to both their goal (*objet*) and their implementation (*mise en œvre*), with the general framework set by the CPP vis-à-vis seizures and with the principles developed by the ECtHR in application of the Convention (Ch. c. Lux., 8 May 2015, n° 1297/15, p. 7).

***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?*

See answer to Q13, explaining that the legal situation is unsettled in Luxembourg regarding consultation/seizures of "distant data". This point was reportedly raised in a case of allegations of *messages désobligeants* (unpleasant messages) sent by one colleague to another. The police searched the residence of the suspect and found a *code secret* on a piece of paper. The police used the code and the email address from which the messages had been sent to access Google Cloud, and copied data. These showed that the suspect had sent similar messages to other colleagues and carefully kept a complete record of their wrongdoing. At the pre-trial hearing, the defence lawyer tried to have the seizure annulled on the grounds that the data were stored on a server in England, and that the police were therefore incompetent to seize them. The tribunal did not examine this argument any further, as the request for annulment was made late: it must come within 5 days of the suspect's being informed of the act (in this case the seizure) (arts 126(3) & 48-2 CPP) (Putz,

2019, p. 169; no reference given for hearing – must be unreported). As noted by Putz, it is possible to argue that when data are copied onto a local medium and then seized, the seizure takes place in Luxembourg. This would be different should the "cloud storage" itself be seized in some sense, e.g. police change the password so that the suspect no longer has access (Putz, p. 250).

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.*

This was partly answered in Q37. The short answer is that the evidence may well be inadmissible under art. 6 ECHR and the related domestic jurisprudence already discussed, but it will be on a case-by-case basis. As already stated, there are no specific legal rules or guidelines for handling digital forensics, but the accused benefits firstly from the very role of the investigating judge whose duty is to be impartial, plus their defence has access to the case file, the right to ask for an expert to be appointed, etc.

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.*

There are no such rules; the pre-trial courts examine these matters on a case-by-case basis, but building on their existing bank of decisions.

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.*

In what is comparatively a very small national jurisdiction, I am not aware of any such case law. Please see following answers for some case law in related areas from which the reasoning may be extrapolated to mobile forensics.

45. **Question:** *Is there in your jurisdiction an established and recognised standardisation(s) of the processes of collection, analysis, interpretation and reporting of digital evidence that must be*

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

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.

This question seems to touch on several others already answered.

***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?*

It may be enough to taint the evidence, leading to its rejection. This was notably the outcome in a different context when the public prosecutor, alleging theft by a cleaner of lunch vouchers and gift vouchers from a bank, attempted to rely on CCTV footage of vouchers being spent at a supermarket (T. A. Lux., 2 July 2014, n° 1872/2014). The CCTV system, however, had not been authorised by the national data protection authority (CNPD) – which constituted a (criminal) *délit* on the part of the supermarket. The public prosecutor's argument that the gravity of the offence by far outweighed that of the illegality committed in obtaining the CCTV footage was rejected by the District Court of Luxembourg, which decided that the violation of legal rules designed to protect the fundamental rights of individuals (in this instance the right to a private life) was clearly more serious than a banal property offence. The Court emphasised that the duty of loyalty in the administration of evidence incumbent upon the public prosecutor must be considered to be the essence of a fair trial, added that other evidence could have been obtained legally by opening a judicial inquiry, and threw out the evidence.

***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.*

Further to my earlier remark on the small size of the jurisdiction, as also set out elsewhere the pre-trial stage usually (judicial inquiry) deals with admissibility and those proceedings are not public. Most such issues in the digital investigations context appear to be settled at the pre-trial stage upon completion of the judicial inquiry. When the pre-trial chamber of the District Court is thus seized by a request for annulment pursuant to Article 126 CPP, the jurisprudence states that the only task of the former is to weigh up whether the investigating judge has (i) failed to fulfil a duty imposed upon her on pain of nullity by the law or (ii) acted in violation of the elementary rights of one of

the parties in such a way as to produce real and important damage (*lésion*) of the essential rights of the parties (Ch. c. Lux., 16 February 2012, n° 551/12; Ch. c. Lux., 2 April 2014, n° 927/14; Ch. c. C., 28 May 2019, n° 494/19).

As far as I am aware there is no such case law on evidence collected through mobile *forensics*. It is perhaps worth mentioning, however, a case concerning evidence originating from a mobile phone which also involved the issue of interplay/cooperation between administrative and judicial authorities.

Any authority, public officer or civil servant etc. which/who becomes aware in the course of its/their duties of facts which are liable to constitute a crime or a felony, must inform the public prosecutor (art. 23(2) CPP). The VAT Administration is also bound to transmit information which may be used in criminal proceedings to the judicial authorities (Article 16(1), Law of 19 December 2008 on cooperation between tax administrations, Mémorial A N° 206). In light of the "free proof" system in Luxembourg, information gathered by any administrative authority may be admissible as evidence in criminal proceedings. Nonetheless, as the general principles apply, evidence must be useful, collected in a loyal manner, and debated adversarially in order to be admitted.

A relevant example of the stringent approach taken by the Luxembourg courts in this regard emerged from proceedings before the correctional chamber of the district court in which the public prosecutor attempted to rely on screenshots (taken on a mobile telephone) which had first been obtained by the customs authority in the course of an inspection (Corr. (*Chambre correctionnelle*), T. A. Lux., 20 December 2017, 493/17 X). First, the court made a literal reading of the above-cited CPP provision binding the customs agents to inform the public prosecutor of their suspicions of criminal wrongdoing, noting that whereas the Code required agents to transmit all information (*renseignements),* reports (*procès-verbaux)* and related acts (notwithstanding any rule of confidentiality or professional secrecy), it did not extend to the obtainment of evidence, which is governed exclusively by the framework of the CPP. Since the public prosecutor had not executed a seizure in accordance with those rules, the evidence was obtained illegally. With that established, the court then applied the strict interpretation of the legality of the administration of evidence established in the 2007 Court of Cassation judgment mentioned above, in order to conclude that the illegally-obtained screenshots violated the right to a fair trial and had to be excluded. The other aspects of the customs agents' report, it having been transferred lawfully, were not excluded.

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

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?*

There is no "certain probative value" given to mobile forensic evidence; nor are there rules or requirements on the interpretation of mobile forensic evidence.

In terms of experts, the functions of the judicial police's SNT specialists in criminal proceedings have already been set out. All other recourse to experts appears to be optional; more precisely, this is decided by the investigating judge during her judicial inquiry. The judge does so by way of a judicial order in which she specifies the information she wishes to obtain from the experts, as well as the questions to which she calls their attention and to which she requests the solution (art. 87(1) CPP). The accused (*inculpé)* may (but without delaying the work of the judge's expert) choose their own expert who is entitled to attend all operations, to address all requests to the experts designated by the judge, and to record his observations on the report of the former in a separate report (art. 87(3) CPP). Should the judge-ordered expertise be made without the *inculpé* being represented, he has the right to choose an expert who will examine the work of the judge-ordered experts and present observations. Should any of these conditions be flouted, a ground for nullity is established (art. 87(7) CPP). The *inculpé,* his advisor and the *partie civile* have the right to request an *expertise* on the facts they indicate, and to ask that the *expertise* ordered by the judge examine those facts. Should the judge refuse, her order must include the reason for the refusal (art. 88 CPP).

Although the *expertise* provisions have generated abundant jurisprudence, none of relevance to mobile forensics or to digital investigations generally was found. A leading investigating judge, commenting in her personal capacity, has stated that recourse to IT experts is in fact never made (by the public side) in practice due to costs concerns (Kraus, 2017, p.230). In the cybercrime context, it was reported in 2017 that the SNT had in the past used specialists from CIRCL (Computer Incident Response Center) Luxembourg, from Europol-EC3 or automated tools from private enterprises for the examination of malware – but presumably without a judicial order

designating an "expert" in the sense of the CPP (GENVAL, 5.2.2). According to an interview with the SNT, recourse to an IT expert by the *inculpé* or defendant is also very rare. Anecdotally, reference was made to one case entailing an independent expert who withdrew his expert analysis once he became aware of the contents of that carried out by the investigators at the SNT. As noted at several places above, the investigating judge may order any person – except the person who is the subject of the judicial inquiry, who retains the right to remain silent – to assist in giving access to seized systems or to data therein or accessible therefrom, as well as in understanding the protected or encrypted data (art. 66(4) CPP). This assistance is mandatory, but unlike in Belgium and France no criminal penalty is foreseen for those who do not comply with the judicial order.

There is no register *per se* for experts, but the website of the Luxembourg Ministry of Justice maintains lists of *experts assermentés,* with a handful self-described as specialising in IT and/or cybercrime (http://mj.public.lu/professions/expert_judicaire/Liste_des_Experts/). According to an interview with the SNT, these experts put themselves onto the lists, and there are no requirements as to qualifications or certifications. It has not been possible to confirm whether the defendant or the subject of the administrative investigation is entitled to check the certificate of independent experts. As noted above, recourse to digital forensics experts would appear to be very rare in practice.

The SNT officers themselves are recruited from outside and trained as police officers, with standard police employment examinations. There are no specific requirements in terms of training or qualifications for the role, but at interview members of the SNT stated that outside training includes that organised by the International Association of Computer Investigative Specialists (IACIS). Training is refreshed and competence re-assessed periodically. At the time of writing, the IACIS website shows 9 members from Luxembourg. Luxembourg is not a member of the European Network of Forensic Science Institutes (ENFSI).

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

No such case law was found.

***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.*

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

Like Q45, this seems to touch on several questions already answered. I would be glad to know if there are specific points envisaged by the question here which I have not addressed.

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

No such case law was found; please see remarks above on the centrality of the pre-trial chambers and the independent, active, supervisory role of the investigating judge.

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

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

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

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

This question also appears to overlap with many earlier questions. I would be glad to address any specific points at interview. One important general point to unpack is that the "equality of arms" is a different proposition in Luxembourg as compared to (especially) adversarial criminal justice systems. The investigating judge is overwhelmingly in control of her judicial inquiry, and is required to search for the truth, following up everything that can inculpate or exculpate.

The CPP provisions set out in the answers here show the centrality of the investigating judge in the management of criminal proceedings entailing digital/mobile forensics and of the judicial police in executing her orders. Whereas the sub-division of powers and duties between those two actors and the public prosecutor is clearly established, the legal framework has minimal interaction with the concrete digital forensics steps taken by investigators on the ground. Indeed beyond the CPP, no rules, soft regulations or checklists of operations are officially prescribed for digital forensics operations – although there is systematic involvement in digital seizures of a specialised "new technologies" police support unit who benefit from outside training. Moreover, in practice it would seem that notwithstanding the absence of a specific legal requirement to do so, investigating judges – who are independent and impartial by design – regularly scrutinise the workings of digital forensics in the course of their judicial inquiries, and through the adversarial dynamics of proceedings before the pre-trial chambers, accepted and censured practices for digital seizures have been gradually distinguished – especially in cases where lawyers are the targets of investigations.

Gauging the potential effects of this legal grey area on the defence is no simple task, not only due to the double-edged role of the investigating judge and the (current) dearth of jurisprudence in what is a small jurisdiction. In particular, further targeted research in the years to come would be required in order to throw light on the "dark figure" of defendants who are not accessing (or even considering accessing) independent digital forensics experts in the course of their defence. The key legal arena for the defence would seem again to be the pre-trial chambers, operating on a case-by-case basis, where it can claim a nullity on both statutory and substantive grounds, such as where the flawed disclosure of evidence imperils the right to a fair trial enshrined in Article 6 of the ECHR. On the one hand, in terms of admissibility Luxembourg combines a free proof system tempered by a strongly-protective approach in the jurisprudence toward illegally-obtained

evidence. On the other, and although full access to the case file is systematically granted to the defence, digital forensics-specific guarantees with regard to disclosure are still missing. The introduction of more detailed legal rules on digital forensics would meet a system which provides ample opportunities to examine levels of compliance with them.

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

No such training is required by law, although it is reported that a handful of prosecutors (three) are specialised in cybercrime along with economic crime in general (Putz, p. 175).

For *magistrats* (encompassing judges, prosecutors, investigating judges), training has been taken from ERA (Academy of European Law, Trier) and Microsoft (focus on cybercrime), and in partnership with the French *École nationale de la magistrature* in Paris, and the *Réseau européen de formation judiciaire* (more general offer) (GENVAL, 8.1.)

***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?*

There is no such requirement.

***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.)?*

This question is **extremely** broad, and also overlaps with many other questions in this file. I would be happy to take any more specific queries.

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?*

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

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

There are no such requirements or guidance.

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.*

This question has already been dealt with in multiple other answers, at both the pre-trial and trial stages.

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

Same answer as above.

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.*

There are no specific legal requirements with regard to information on the rights granted to subjects for mobile forensics or digital investigations more broadly. Nor are there specific legal requirements with regard to aspects of the report of the procedure of digital investigations which must be disclosed to the subject, or any procedural right to gather evidence conferred on subjects in Luxembourg law. The underlying reason for the latter lies in the central role assigned in inquisitorial systems to the investigating judge, who has a statutory duty to search for the truth using powers to gather both inculpatory and exculpatory evidence. The accused is, however,

generally free to carry out any act that may boost his defence – except coercive measures – and there is in principle no limitation on evidence which may be admitted at trial. In principle, digital investigations carried out by the defendant have evidentiary value; since Luxembourg uses a "free proof" system, any type of evidence is *a priori* admissible before the criminal courts (see further Section 4 immediately below). It is however essential that evidence be useful, "loyally" obtained, and subject to the adversarial principle (*contradictoire*). For example, unilateral expert reports are admissible so long as the parties have the opportunity to freely discuss them (Ch. c. C., 6 December 2013, N° 699/13).

As stated above, although full access to the case file is systematically available to the defence there are no digital investigation-specific guarantees with regard to disclosure. Given the lack of relevant statistics and the relative dearth of case law (in turn partly due to the centrality of the investigating judge and of pre-trial hearings, which are not public) in what is a small-sized criminal justice system, further targeted research in the years to come would be required in order to make informed observations as to the critical issues concerning the disclosure of digital data, and to shed light for instance on the "dark figure" of defendants who are not accessing (or even considering accessing) independent digital forensics experts in the course of their defence. The key legal arena for the defence would seem to be the pre-trial chambers, where it can claim a nullity before on both statutory and substantive grounds, such as where flawed disclosure of evidence imperils the right to a fair trial enshrined in Article 6 of the ECHR. Assessment by the chambers is performed on a case-by-case basis, in a grey area lacking tailored procedural rules for digital investigations, which impedes the drawing of general conclusions with regard to the effectiveness of such remedies.

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.*

The entire process, whether *enquête* or *instruction,* is subject to secrecy (art. 8(1) CPP), whilst pre-trial hearings are not public. Regarding expert witnesses, please see answer to Q48 above.

Potentially relevant to witnesses: since 2018, a third party with a legitimate personal interest can appoint an expert. This amendment was deemed necessary in order to redress an imbalance revealed by criminal proceedings in which the *expertise* employed by the *inculpé* had led to a third party being suspected of criminal wrongdoing and then, in turn, being *inculpé*. Whereas third

parties already had the power (under Article 126 of the CPP) to request the nullity of an *expertise* concerning them, the reform extended the third party's right to make a request to the investigating judge to have their own expert engaged (*Projet de loi* n° 7720, *Exposé des motifs,* p. 12).

(Included here as there is no separate question for third parties). Article 68(1) of the CPP also enables third parties to request restitution, whilst under Article 67 the investigating judge may order on her own motion and at any moment the total or partial release (*mainlevée*) of seized data. At interview, members of the SNT stated that this power is used regularly, where data are not of an illegal nature, in particular to relieve the burden on small businesses which would struggle to continue operating without access to their main devices and/or data.

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.*

As noted above, the investigation and the *instruction* are subject to secrecy (art. 8(1) CPP). There are many other provisions in Luxembourg law – constitutional and secondary legislation – which prohibit breaches of privacy (see answer to Q5).

Luxembourg has implemented Directive 2012/29/EU on victims of crime (Law of 8 March 2017, Mémorial A346). The victim can request interpretation and translation (arts 3-4 & 3-5 CPP), they must be informed of their rights (e.g. to demand reparations) in a language they understand; depending on the needs of the victim, supplementary information may be provided to them at each stage of the procedure (art. 3-7). The victim receives on demand information on the state of the criminal procedure unless this notification may harm the progress of the case (art. 4-1(4)). If the victim has become *partie civile*, they may attend searches and seizures (art. 63(2) CPP) and request the appointment of an expert on indicated facts (art. 88(1)).

Although there is no procedural right to access the entire public dossier, it is reportedly not uncommon for victims of computer crimes to bring their own detailed dossier to the police or to actively cooperate with police authorities during the investigation (Putz, 2019, p. 218); it may even be possible for the victim to have fees paid to cyber-detectives reimbursed by the convicted person(s) (CSJ, 26 novembre 2014, no. 512/14 X). Companies in particular provide technical reports from the internal IT department or external experts, or logs from the time of a cyber-attack. The case law holds that this evidence is presumed reliable; if the accused affirms that they have been manipulated, they must provide some proof of this. At the same time, these analyses are usually pre-verified by the SNT of the Judicial Police (Putz, 2019, p. 219).

FORMOBILE

• FROM MOBILE PHONES TO COURT •

formobile@netlaw.bg

Linkedin – Formobile-

Twitter – @Formobile2019

www.formobile-project.eu

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

Section 6: Comments

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

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

No further comments; in Q52, I provided an overview of sorts of the situation in Luxembourg regarding digital investigations in general – but little information is available on mobile forensics.