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

## IMPORTANT TO READ BEFORE ANSWERING THE QUESTIONNAIRE:

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

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

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

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

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

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

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

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

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

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

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

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

## Introductory questions:

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

**Answer:** Inthemis, executive director.

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

**Answer:** Montpellier, France.

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

**Answer:** French law does not define the expression "mobile device". The Penal Code, the Penal Procedure Code and the Internal Security Code evoke the notions of "terminal equipment" and of 'Automated Data Processing System", the latter expression corresponding to the notion of "Computer system" of the Budapest Convention on Cybercrime of the Council of Europe.

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:*

*Subsection I - Mobile device not seized*

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

The Penal Procedure Code (PPC) does not provide for the possibility to access a technical device, including mobile phones, outside the search and seizure procedure. For consistency reasons, search and seizure will be described together in the next subsection (indeed, the seizure of the device or of certain data only will solely be based on casuistic reasons) and will only be here evoked additional procedural powers.

The PPC provides for several powers that enable investigators to access electronic evidence without accessing or seizing the device. These powers might be exercised whatever the computer system at stake (including mobile phones).

(1) Remote data capture (Articles 706-102-1 to 706-102-9 of the Penal Procedure Code - procedure to be followed is established in Articles 706-95-11 to 706-95-19 of the PPC - Provisions are exhaustively translated in Appendix).

(2) Collection of connection data and interception of correspondence by using a technical device (Art. 706-95-20 of the Penal Procedure Code – procedure to be followed is

established in Articles 706-95-11 to 706-95-19 of the PPC - Provisions are exhaustively translated in Appendix).

(3) Interception of correspondence and remote access to correspondence stored by means of electronic communication, accessible using an electronic identifier (Arts. 706-95 to 706-95-3 of the Penal Procedure Code - Provisions are exhaustively translated in Appendix).

**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?*

Limits are the respect of the rules set-up in the Penal Procedure Code, including:

- The need for a link with a felony (access to correspondence with an electronic identifier) and/or organised crime (correspondence intercept, remote data capture and collection of connection data and interception of correspondence by using a technical device),
- An authorisation issued by a magistrate (all offences), which must be reasoned (all offences: Art. 100-1 PPC in relation to correspondence interception; arts. 706-95-1 and 706-95-2 PPC in relation to access to correspondence using an identifier; art. 706-95-13 in relation to the other powers of procedure).
- A special protection of advocates, magistrates, member of the Parliament and senators (correspondence interception: Arts 100-7 and 706-95 PPC; access to correspondence by using an identifier: Arts. 100-7 and 706-95-3 PPC; remote data capture: Art. 706-102-5 PPC; collection of connection data and interception of correspondence by using a technical device: Article 706-95-20).
- The fact that sequence relating to private life and that has no relation with penal infringements mentioned in the decisions that authorise the measure can be kept in the criminal case file (only in case of remote data capture and of collection of connection data and interception of correspondence by using a technical device: article 706-95-18 PPC).

Further details may be found in the provisions included in the Appendix.

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

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

Once data are collected, investigators may have recourse to qualified persons or to technical tools in order to decrypt the collected information (arts 230-1 to 230-5 PPC). They may also have recourse to the means of the State covered by National Security where needed, under the district prosecutor or the investigating judge supervision (Article 230-2).

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

Intercepted information can be copied (see provisions in the Annex).

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

Powers of procedure mentioned in this subsection are implemented without the owner/possessor consent. However Article 100 PPC enables to intercept correspondence on the line of the victim for any misdemeanour punished by imprisonment if this victim gives his/her consent to it.

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

This question will only be relevant within the framework of the search and seizure procedure (See below).

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

Powers of procedure mentioned in this subsection are implemented without the owner/possessor knowledge.

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

The implementation of a power of procedure described in the current subsection is decided, in case of preliminary or flagrancy procedure, by the liberty and custody judge of the district court at the request of the district prosecutor, and in case of judicial information, by the investigative judge.

Formal requirements are available in the provisions that are translated in the Annex. Mainly, these powers may only be exercised in relation to organised crime, at the exception of the power to access to correspondence with an electronic identifier, which may also be used within the framework of an investigation on any felony. Authorisation decisions must be reasoned and official records of operations must be drawn-up. Moreover, operations cannot, under penalty of nullity, pursue another purpose than that of investigating and detecting penal infringements that are mentioned in the decision of the magistrate. In addition, within the framework of the interception of correspondence by using a technical device, correspondence intercepts can only relate to the person or to the communication link referred to in the authorisation of interception. Finally, authorisations to exercise powers of procedure described in the current Subsection are subject to maximal durations (correspondence interception: one month, renewable once under the same conditions of duration; remote data capture: one month renewable once where authorised by the liberty and custody judge, and four months renewable, without the total period of operations being longer than two years, where authorised by the investigative judge; collection of connection data and interception of correspondence by using a technical device: forty-eight hours renewable once.

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

The PPC is silent on this issue. The line or the device on/from which data are intercepted may be the one of any person, as soon as there is a need to carry out such interception in order to conduct the investigation, provided that other conditions provided for in the PPC are respected.

***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.*

I answer this question in the following Subsection dedicated to search and seizure. As regards powers described in the current Subsection, only correspondence interception and remote access to correspondence using an identifier could be concerned.

In relation to correspondence interception, Art. 100-8 of the PPC states the following[1]:

> *Article 100-8:*
>
> *Where an interception of correspondence transmitted by means of electronic communication targets an address of communication which is used on the territory of a Member State of the European Union, whereas it does not take place within the framework of a European investigation order, the investigating judge or the judicial police officer appointed by him notifies this interception to the competent authority of this State where the person concerned is located on its territory.*
>
> *This notification shall take place either before the interception where it appears from the elements contained in the record of the proceedings at the time the interception is ordered, that the targeted person is or will be on the territory of this State, or during the course of the interception or after it has been made, as soon as it is established that the targeted person is or was on this territory at the time of interception.*
>
> *Upon request by the competent authority of the Member State, made within ninety six hours from receipt of the notification and justified by the fact that such interception could not be authorised, within the framework of a similar national proceeding, under the law of that State, either the interception cannot be carried out or it must be interrupted, or intercepted data while the person was on its territory cannot be used and must be removed from the record of the proceedings or can be used only under the conditions specified by this authority and for the reasons it specifies.*
>
> *The absence of the act of notification provided for in the first and second paragraphs is considered to be a cause for nullity of proceedings only where it is established that such interception could not be authorised within the framework of a similar national proceeding, under the law of the Member State on whose territory was the targeted person.*

[1] This translation corresponds to the update, made by the author of the current report, of the translation of the PPC proposed on the French legal portal "Legifrance" and dated from 2005, which was until recently available at https://www.legifrance.gouv.fr/content/location/1741 from https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations.

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

In relation to remote access to correspondence using an identifier, Articles 706-95-2 and 706-95-2 PPC do not regulate the case where the mailbox is stored in another country than France. As a result, is supposed be followed the procedure for international judicial cooperation stated in Arts. 694 *et seq.* of the PPC (unless investigators access the content of a mailbox within the framework of a search and seizure procedure – in this case they may access emails stored abroad without having recourse to judicial cooperation - see the answer under Question n° 25). These provisions apply in the absence of any international convention or bilateral treaty stipulating otherwise[2].

Within the limits of the provisions of these articles, and within the limits of the powers for accessing electronic communications set out in the French Penal Procedure Code, including article 100-8 which regulates some transborder situations[3], mutual legal assistance may enable real-time access to electronic communication data.

A first chapter dedicated to general provisions regulates the transfer and execution of judicial assistance requests (articles 694 to 694-4-1), assistance for the purpose of hearing, surveillance and infiltration (articles 694-5 to 694-9), and judicial assistance for the purpose of seizure of the proceeds of penal infringements with a view to subsequent confiscation (articles 694-10 to 694-13).

A second chapter dedicated to the provisions that are specific to judicial assistance between France and the other EU member States regulates European investigation orders (articles 694-15 to 694-50), joint investigation teams (articles 695-2 to 695-3), the EUROJUST unit (articles 695-4 to 695-7), the EUROJUST national representative (articles 695-8 and 695-9), the issue and execution of orders freezing property or evidence (articles 695-9-1 to 695-9-30), simplified exchange of information between services in application of the framework decision of the EU Council of 18 December 2006 (articles 695-9-31 to 695-9-49), cooperation

[2] Art. 694 PPC.
[3] See the Appendix of the current report, A.

between Asset Recovery Offices of Member States in the area of tracing and identifying proceeds of crimes and other goods in relation to crime, in application of Decision 2008/845/JHA of the Council of 6 December 20017 (articles 695-9-50 to 695-9-53), and the prevention and resolution of conflicts of competence exercised in application of the framework decision of the Council of the European Union of 30 November 2009 (articles 695-9-54 to 695-9-57).

A third Chapter contains one provision pertaining to judicial assistance between France and certain States (article 695-10).

A fourth Chapter contains provisions regulating the European arrest warrant, procedures for transfer between Member States resulting from the EU Council framework decision of 13 June 2002 and procedures for transfer resulting from agreements concluded by the European Union and other States (articles 695-11 to 695-58).

In addition, France has ratified the Council of Europe Convention on cybercrime with two reservations in relation to the procedure. Firstly, "France reserves itself the right not to establish jurisdiction when the offence is committed outside the territorial jurisdiction of any State"[4]. Secondly, France declared that "whenever the offence is punishable under criminal law where it has been committed, proceedings shall be instituted only upon request from the district prosecutor and must be preceded by a complaint from the victim or his/her beneficiaries or by an official complaint from the authorities of the State where the act was committed"[5].

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

[4] Council of Europe, Reservations and Declarations for Treaty No.185 - Convention on Cybercrime, France, status as of 18/02/2019, available at https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/declarations?p_auth=DVkVUK3n&_coeconventions_WAR_coeconventionsportlet_enVigueur=false&_coeconventions_WAR_coeconventionsportlet_searchBy=state&_coeconventions_WAR_coeconventionsportlet_codePays=FRA&_coeconventions_WAR_coeconventionsportlet_codeNature=2.

[5] *Ibid.*

Yes, an answer to this question has already been brought under Question n°5: powers described under the current Subsection can only be exercised:

- In case of felony as regards access to correspondence with an electronic identifier;
- In situations of organised crime (offences to be included in the latter notion are listed in Articles 706-73 and 706-73-1 PPC) as regards correspondence interception, remote data capture and collection of connection data and interception of correspondence by using a technical device.

***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.*

Evidence that is collected in violation of the requirements established in the Penal procedure Code cannot be used in the proceedings where the latter Code provides explicitly for such penalty or where it provides for the nullity of the procedure of data collection or interception[6]. Where the Code is not clear on this issue, the inadmissibility of evidence may be decided by the judge upon request of the interested party.

The Court of Cassation established a requirement of fairness of evidence, as a condition for the exercise of the rights of the defence, and, more generally, as a condition for a fair trial.[7]

However, this requirement is more strictly enforced in relation to evidence produced by the public authority (or by a private party on the instructions of the public authority), in comparison with evidence produced by a private party.

---

[6] See the Appendix for the extensive content of provisions.

[7] Pascal Lemoine, "La loyauté de la preuve (à travers quelques arrêts récents de la chambre criminelle)," Cour de cassation annual report 2004, available at https://www.courdecassation.fr/publications_26/rapport_annuel_36/rapport_2004_173/deuxieme_partie_tudes_documents_176/tudes_diverses_179/travers_quelques_6401.html#n_20_. See also Haritini Matsopoulou, Consécration et limites du principe de loyauté de la preuve : quelle réalité ? Le point de vue du professeur (Consecration and limits of the principle of evidence fairness : which reality ? The point of view of a Professor), 27 August 2019, Actualités du droit, https://www.actualitesdudroit.fr/browse/penal/procedure-penale/23386/consecration-et-limites-du-principe-de-loyaute-de-la-preuve-quelle-realite-le-point-de-vue-du-professeur.

Evidence produced by public authorities may be the result of certain positive acts, but it must not be the result of acts that caused the author to commit a penal infringement, in other words these acts must not have provoked or incited the commission of the penal infringement that is being proven.[8] More widely, the Court of Cassation rejects evidence obtained by fraudulent means.[9] Evidence thus obtained will be declared inadmissible,[10] and may even result in the nullity of proceedings.[11]

However, the Court of Cassation does accept acts of provocation that are not at the origin of the penal infringement, but which enable the infringement to be proven.[12]

In addition, it is to be noted that the PPC authorises judicial police officers and agents to commit certain penal infringements, for the purpose of the repression of certain misdemeanours and felonies. *Inter alia*, in relation to organised crime and attacks on automated data processing systems, these officers and agents may participate in electronic discussions with persons who are likely to have committed an infringement and may gather evidence of this infringement within this framework.[13]

---

[8] Cass. crim., 27 Feb. 1996, "Schuller" court case, bull. crim. 1996, n° 93; JCP 96, ed. G, II-22629, note M.-L. Rassat; D. 96, p. 346, note Ch. Guéry; Cass. crim., 11 May 2006, pourvoi n°05-84.837, bull. crim. 2006, n°132; see Pascal Lemoine, *op. cit*. See also Cour de cassation, rapport annuel 2012, *La preuve*, Livre 3, partie 4, Titre 2, Chapitre 2 – Admissibilité des modes de preuve, available at https://www.courdecassation.fr/publications_26/rapport_annuel_36/rapport_2012_4571/livre_3_etude_preuve_4578/partie_4_administration_preuve_4589/principes_gouvernant_4591/admissibilite_modes_26241.html

[9] Cass. crim., 28 Oct. 1991, bull. crim., n° 381; JCP, 1991.II.21704, note J. Pannier.

[10] Cass. crim., 9 Aug. 2006, n° 06-83.219, bull. crim. 2006, n° 202; Cass. crim., 7 Feb. 2007, pourvoi n° 06-87.753, bull. crim. 2007, n° 37; Cass. crim., 4 June 2008, pourvoi n° 08-81.045, bull. crim. 2008, n° 141; see Cour de cassation, rapport annuel 2012, *La preuve, op. cit*.

[11] Cass. crim., 27 Feb. 1996, bull. crim. 1996, n° 93.

[12] Cass. crim., 30 April 1998, pourvoi n° 97-85.747, bull. crim. 1998, n° 147; Cass. crim., 8 June 2005, pourvoi n° 05-82.012, bull. crim. 2005, n° 173; Cass. crim., 16 Jan. 2008, pourvoi n° 07-87.633, bull. crim. 2008, n° 14; see Cour de cassation, rapport annuel 2012, *La preuve, op. cit*.

[13] Article 706-87-1 PPC.

In any case, a prerequisite for the admissibility of evidence is that the produced evidence is submitted to a debate between parties. This principle is established in the PPC[14] and is recalled by the Court of Cassation, particularly where it does accept the admissibility of some proof obtained by illicit or unfair means, in order to ensure that such proof does not entail a breach of the rights of defence[15].

This implies that each of the parties can access the evidence produced by the other parties and has the time and the right to challenge this evidence[16]. As a result, the accused is empowered to challenge the means used and the procedure that has been followed in order to intercept electronic communications.

This being said, the legal admissibility of evidence does not prejudge its probative value, which is partly regulated in the Penal Procedure code and the Civil Code in relation to electronic writing.

- *Inter alia*, according to the Civil Code, a writing consists of letters, characters, figures or of any other sign or symbol endowed with an intelligible meaning, whatever its supports. Electronic writing has the same probative value as paper-based writing, provided that the person from whom it originates can be duly identified and that it is established and stored in a manner capable of assuring its integrity. The signature which is necessary to complete a legal act identifies the person who places it on the document. It demonstrates their consent to the obligations which arise from the act. Where it is placed on the act by a public official, it confers authenticity on it. Where it is in electronic form, it consists of the use of a reliable

[14] Art. 427 PPC related to the production of evidence before the penal court judging misdemeanours, according to which evidence must be presented to the judge during court proceedings and be contradictorily discussed before them. Other parts of the PPC regulate specifically the production of evidence before the different courts: see especially arts. 278 s. in relation to the Assize Court, which provide *inter alia* for the possibility, for the advocate, to access all documents relevant to the proceedings (art. 278), and which clarifies that the judge must concisely elaborate evidence of charge and discharge during the course of the hearing (art. 327).
[15] See Court of cassation, rapport annuel 2012, *La preuve, op. cit*.
[16] This is especially organised in arts. 400 s., 427 s. and 458 s. PPC in relation to the judgment of misdemeanours and in arts. 283 s., 306 s. and 323 s. PPC in relation to the judgment of felonies.

process of identification, guaranteeing its link with the legal act to which it is attached. The reliability of the process is presumed, in the absence of proof of the contrary, where the electronic signature is created, the identity of the signatory is ensured, and the integrity of the legal act is guaranteed, under the conditions laid down by decree in Council of State. Where the law has not laid down other principles, the judge settles conflicts between written evidence by determining, using any means, which is the more convincing instrument.

- According to the Penal Procedure Code, a police record has probative value only if its form complies with legal requirements and if its author acted in the performance of their duties, on an issue falling within the scope of their responsibilities, and if they reported what they saw, heard, or noticed personally.

Proof to the contrary can in principle be established by any means, unless the law states otherwise, which is the case in very few matters (for example, where police records have been established by police officers or agents who received from a special legal provision the power of recording misdemeanours through police records, evidence to the contrary can only be produced in writing or by testimony[17]). Moreover, some special laws set out that some particular official records are considered to be valid proof until specific proceedings are launched to challenge the authenticity of facts[18], but this does not concern the powers described in the current Subsection. Finally, written proof cannot result from correspondence between the accused and their lawyer,[19] and the court can always order a forensic examination, if deemed necessary[20], as well as complementary investigations[21].

Beyond these particular types of evidence, the authenticity and integrity of evidence may always be challenged. Where investigators do not have the sufficient expertise in order to

[17] Art. 431 PPC.
[18] Art. 433 PPC.
[19] Art. 432 PPC.
[20] Arts. 434, 310 PPC.
[21] Arts. 283, 436 and 456 PPC.

preserve evidence's authenticity and integrity, they may have recourse to Article 60-3 PPC, applicable to flagrancy investigations but also preliminary investigation[22] and judicial information[23]. Article 60-3 PPC states that where have been sealed objects that are computer data storage medium, investigators may, by any means, require any qualified person registered on one of the lists provided for in Article 157 PPC or having swear in writing the oath provided for in Article 60 PPC, to carry out the opening of judicial seals in order to make one or several copies of the data so that they can be used without undermining their integrity. The required person mentions operations that have been carried out in a report established in compliance with Articles 163 and 166.

In addition, there is a security standard in France, *inter alia* applicable to interrelations between administrations and citizens and aiming at creating confidence of the latter in administrative electronic services, calls RGS[24]. The RGS which set-up guidelines aiming at preserving the security of information systems, including information's integrity. Its respect is of a nature to strengthen the reliability of stored information (provided their authenticity has been preserved and the way they have been handled from their collection can be demonstrated).

## *Subsection II - Search and seizure of the Mobile device or of Mobiles'data*

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

Yes, as any device. Alternatively the device can be accessed during a search operation and may be solely seized the data that are discovered and that are useful to the investigation.

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

[22] Article 77-1-3 PPC.
[23] Article 99-5 PPC.
[24] Référentiel général de sécurité, which means « general security standard ». See https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/.

Search and seizure of information held by a third party is set out in articles 76 to 76-3 (preliminary investigation), 56 to 59 (flagrancy investigation), 92 to 99-4 (investigation procedure conducted by an investigative judge), and 706-89 (in relation with a limited list of crime or misdemeanours) of the Penal Procedure Code.

This general procedure, performed by a judicial police officer or an investigating judge depending on the procedure that is followed (preliminary or flagrancy investigation in the first case, judicial information in the second case)[25], is applicable to computer data that is of interest for the investigation and that is stored (1) in computer systems in the places that are searched, (2) in computer systems that are connected to these latter systems (as long as this data is accessible from or for the initial system[26]), (3) and in computer systems that are connected to systems located on the premises of a unit or a service of the Police or of the Gendarmerie, in compliance with rules governing search, as long as this data is accessible from the initial system[27]).

Where it is established in advance that this data, accessible from or for the initial system, is stored in a computer system that is located outside the national territory, it is collected subject to conditions of access under applicable international commitments.[28] Collected data may be copied onto any support, and digital supports may be seized and placed under seals under the conditions set out by the Penal Procedure Code.[29]

Formal requirements are different from those surrounding the powers of procedure evoked in the previous Subsection, since the impact of search and seizure on privacy is considered as being lower. As a result, the procedure of search and seizure can be used within the framework

[25] Arts. 56, 76 and 94s. PPC.
[26] Article 57-1 PPC (relating to flagrancy investigations). See also (for the application of the same rules within the framework of preliminary investigations and judicial information) articles 76-3, 97 and 97-1 PPC.
[27] Article 57-1, §2 PPC.
[28] Article 57-1, §3 PPC.
[29] Article 57-1, §4 PPC.

of any investigation on a felony or a misdemeanour, and is not limited to the investigation of certain kinds of penal infringements only.

Formal requirements include:

-The possibility to carry-out a search is limited, within the framework of flagrancy[30] and preliminary[31] investigations, to the home of persons who appear to be involved in the penal offence under investigation or to be in possession of documents, information or articles pertaining to this offence. Within the framework of a judicial information, searches can be made in "all the places where may be found objects or computer data which could be useful for the discovery of the truth" [32].

-The express hand-written consent of the person in whose residence the operation takes place in case of a preliminary investigation only (this consent may be bypassed by a written and reasoned decision of the liberty and custody judge made at the request of the district prosecutor, if the needs of an inquiry into a felony or a misdemeanour punished by a prison sentence of three years or more justifies it)[33]. The consent of this person is not required in the other cases (flagrancy investigation and judicial information), but the operations must be made in the presence of the person in whose domicile the search is made and where this is impossible, the judicial police officer has the duty to ask him or her to appoint a representative of his choice; failing this, the judicial police officer will appoint two witnesses, chosen for this purpose from among persons who are not under his administrative authority.[34]

[30] Article 56 PPC.
[31] Article 76 PPC, which calls to the application of Article 56 PPC.
[32] Article 94 PPC. This translation correspond to the translation of the PPC proposed on the French legal portal "Legifrance" and dated from 2005, which was until recently available at https://www.legifrance.gouv.fr/content/location/1741 from https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations, updated where needed by the author of the current report.
[33] Article 76 PPC.
[34] Article 57 PPC, Articles 95 and 96 PPC.

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

- The judicial police officer (flagrancy, preliminary investigation) or the investigating judge (judicial information), is the only person, together with the persons mentioned in the previous paragraph and any persons upon whom he or she calls pursuant to article 60 in order to provide technical or scientific assistance, to be allowed to examine the papers or documents or computer data before proceeding to seize them. He or she has the duty first to initiate any step appropriate to ensure the observance of professional secrecy and of the defendant's rights, without prejudice to the application of Articles 56-1 à 56-5 PPC[35], and he or she must draw up an official report of operations[36].[37]

- Is only allowed the seizure of objects, documents or computer data useful for the discovery of the truth[38].

- Any article or document seized is immediately entered on an inventory and placed under official seals. However, if it is difficult to make such an inventory on the spot, they are put under temporary closed official seals until such time as an inventory can be taken and they can

[35] Articles 56-1 to 56-5 PPC organise special protection, respectively, for lawyers/barristers (a search at their home or office can only be carried out by a magistrate in the presence of the Bar President or his delegate and pursuant a written and reasoned decision taken by this magistrate, the magistrate and the Bar President are the solely persons who can consult documents before their seizure and the seizure cannot include documents or objects that relate to other infringements that are not mentioned in the above-mentioned decision – all these requirements being decreed under penalty of nullity; the Bar President or his delegate may oppose the seizure of a document or of an object, which will be settled by the liberty and custody judge), for press enterprises and journalists (a search at their home or office and cars can only be carried out by a magistrate, other rules being *mutatis mutandis* the same as those concerning lawyers), for medical doctors, notaries and bailiffs (a search at their office can only be carried out by a magistrate in the presence of the person responsible for the order or professional organisation to which the person concerned belongs, or its representative – Art. 56-3 PPC does not include any other derogations); in places identified as hosting information covered by national security (search can only be carried out by a magistrate in the presence of the President of the Commission of national security secrecy, other rules being mostly, *mutatis mutandis*, the same as those concerning lawyers), and for Courts facility and home of persons who exercise judicial functions where the search aims at seizing documents that are likely to be covered by deliberation secrecy (search can only be carried out by a magistrate in the presence of the First President of the Court of Appeal or the First President of the Court of Cassation or its delegate, other rules being mostly, *mutatis mutandis*, the same as those concerning lawyers).

[36] Article 56, 57 and 66 PPC, Article 76 PPC; Article 96 PPC

[37] In relation to the whole paragraph, see Article 56 PPC, Article 76 PPC; Article 96 PPC.

[38] Articles 56, 76 and 96 PPC.

be placed under final official seals. This is done in the presence of the persons who have witnessed the search pursuant to the conditions set out by article 57.[39]

- The seizure of any computer data necessary for the discovery of the truth is carried out by placing in the hands of justice, either the physical medium holding this data or a copy of the data made in the presence of those persons present at the seizure.[40] If a copy is made, then on the orders of the district prosecutor (flagrancy or preliminary investigation)[41] or of the investigating judge (judicial information)[42], any computer data the possession or use of which is illegal or dangerous to the safety of persons or property may be permanently erased from any physical medium that has not been placed in judicial safekeeping. With the agreement of the district prosecutor (flagrancy or preliminary investigation)[43] or of the investigating judge (judicial information)[44], the judicial police officer only allows the seizure of articles, documents or computer data useful for the discovery of the truth.

- Except where they are requested from within a building or in the exceptional cases provided for by law, searches and house visits may not be undertaken before 6 a.m. or after 9 p.m. [45]

- Particular requirements are provided for in case the search involves information covered by national security secrecy[46] or certain kind of persons (advocates, media companies, audio-visual communication companies, online public communication companies, press agencies, journalists, doctors, notaries, bailiffs, judges[47]).

- Within the framework of flagrancy investigations and judicial information, and subject to the requirements of inquiries or judicial investigations, any communication or disclosure made

[39] In relation to the whole paragraph, see Articles 56, 76, 97 PPC.
[40] Articles 56, 76 and 97 PPC.
[41] Articles 56 and 76 PPC.
[42] Article 97 PPC.
[43] Articles 56 and 76 PPC.
[44] Article 97 PPC.
[45] Article 59, 76 and 96 PPC.
[46] Art. 56-4 PPC.
[47] Articles 56-1 to 56-3 and 56-5 PPC.

without the authorisation of the person under judicial examination or that of his beneficiaries or of the signatory or addressee of a document found during a search, to a person not authorised by law to examine it, is punished by a maximum of €4,500 fine and two years' imprisonment[48].

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

Yes.

**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?*

Limits have been exposed under question n° 17.

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

As explained under question n°17, consent will only be required within the framework of preliminary investigations.

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

Articles 57-1, 76-3 and 97-1 PPC[49] empower judicial police officers to, by any means, require any person who is likely (1) to have knowledge of measures applied in order to protect the data to which it is authorised to access within the framework of the search; and (2) to provide them with information that enable to access data mentioned in §1°. With the exception of

[48] Articles 58 and 98 PPC.
[49] Article 57-1 PPC relates to flagrancy investigations. Same rules are applicable to preliminary investigations and judicial information as stated in articles 76-3 and 97-1 PPC.

persons referred to in articles 56-1 to 56-5[50], refraining from responding as soon as possible to this requisition is punished by a fine of 3 750 €.

However, this provision does not apply to the accused person, who has the right to silence and a right against self-incrimination.

This being said, both afore-mentioned rights have been slightly weakened by a provision that has been created in the Penal Code (PC), in a Section entitled "Obstructing the course of justice": Article 434-15-2 PC.

Article 434-15-2 PC states that "a penalty of three years' imprisonment and a fine of €270,000 are incurred by anyone who, having the key to decipher an encrypted message which may have been used to prepare, facilitate or commit a felony or a misdemeanour, refuses to disclose that key to the judicial authorities or to operate it following instructions issued by the judicial authorities under of title II and III of Book I of the Code of Criminal Procedure. Where the refusal was made where the disclosure of the key or its operation would have prevented the commission of a felony or a misdemeanour or would have limited its consequences, the penalty is increased to five years' imprisonment and a fine of €450,000" [51].

The above-mentioned penal offence should not apply to the person accused, since it appears to be contrary to the rights to silence and against self-incrimination. However, the Constitutional Council is not of this opinion, even though it restricted the possibility to

[50] Articles 56-1 to 56-5 PPC organise special protection, respectively, for lawyers/barristers, for press enterprises and journalists, for medical doctors, for notaries and bailiffs, in places identified as hosting information covered by national security, and for Courts facility and home of persons who exercise judicial functions where the search aims at seizing documents that are likely to be covered by deliberation secrecy. See Appendix, search and seizure, Art. 56 PPC.

[51] This translation correspond to the update, made by the author of the current report, of the translation of the PC proposed on the French legal portal "Legifrance" and dated from 2005, which was until recently available at https://www.legifrance.gouv.fr/content/location/1740 from https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations.

penally sanction the accused persons who refused to provide investigators with the information that enables to access their personal information.

By decision of 2018, the Constitutional Council stated:

-An encryption key may be asked "only if this cryptology means is likely to have been used in order to prepare, facilitate or commit a felony or a misdemeanour[52], and only if the request is issued by the judicial authority"[53]. "In order to obtain the encryption key, investigators must therefore demonstrate before a judge that the content will be useful to the inquiry"[54].

-The penal Code establishes only the obligation, for the person who is accused to have committed a penal offence using an encryption mean, to provide for or to apply the encryption key if he or she does know it[55]. As a result, where the investigator cannot demonstrate that this person is aware about the mean to decipher the content, he or she cannot force this person to deliver or apply the key[56].

On April 2019, the Court of Appeal of Paris[57] confirmed that the offence described in Article 434-15-2 PC cannot be established against a person accused if his or her assistance to access his or her information was not required by a judicial authority (in the present case it was requested by an investigator during the hearing of the accused person).

Moreover, by the same ruling, the Court of appeal considered that a mobile phone unlock code enables to access to data that are on the mobile, including potential messages received in

[52] Constitutional Council, Decision n°2018-696 QPC of 30 March 2018, Recital n°7 (see also Recital n°8), https://www.conseil-constitutionnel.fr/decision/2018/2018696QPC.htm.
[53] Constitutional Council, Decision n°2018-696 QPC of 30 March 2018, *op. cit.*, Recital n°7.
[54] Translated from French. Guénaël Pépin, Le Conseil constitutionnel impose de passer par un juge pour obtenir les clés de chiffrement (The Constitutional Council imposes to involve a judge in order to obtain encrytion keys), 30 March 2018, Next Inpact, https://www.nextinpact.com/article/28222/106391-le-conseil-constitutionnel-impose-passer-par-juge-pour-obtenir-cles-dechiffrement.
[55] Constitutional Council, Decision n°2018-696 QPC of 30 March 2018, *op. cit.*, Recital n°8.
[56] *Ibid*.
[57] CA Paris, 16 April 2019, n° 18/09267, https://www.doctrine.fr/d/CA/Paris/2019/UAD7B86AAE3CD2E367D98.

it, but that such a code does not enable to decrypt messages that have been encrypted, and in this sense that it does not constitute an encryption key. As a result, accused persons may refuse to unlock their mobile phone without committing the offence described in Article 434-15-2 PC.

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

Yes, as explained under question n°17, the person in whose domicile the search is made must be present and where this is impossible, this person must be put in a position to appoint a representative of his choice; failing this, must be appointed two witnesses, chosen for this purpose from among persons who are not under the investigator's administrative authority.

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

Yes, and judicial police officers may, by any means, require any person who is likely:

1° To have knowledge of measures applied in order to protect the data to which it is authorised to access within the framework of the search;

2° To provide them with information that enable to access data mentioned in §1°.

With the exception of persons referred to in articles 56-1 to 56-5, refraining from responding as soon as possible to this requisition is punished by a fine of 3 750 €.[58]

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

No, within the framework and limits described under question n°17.

**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*

[58] Articles 57-1, 76-3 and 97-1 PPC. This translation corresponds to the update, made by the author of the current report, of the translation of the PPC proposed on the French legal portal "Legifrance" and dated from 2005, which was recently available at https://www.legifrance.gouv.fr/content/location/1741 from https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations.

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

*European Investigation Order or Mutual Legal Assistance Treaties the only route or do other options exist? Please elaborate.*

As explained under Question n° 17, may be searched computer data that is of interest for the investigation and that is stored (1) in computer systems in the places that are searched, (2) in computer systems that are connected to these latter systems (as long as this data is accessible from or for the initial system[59]), (3) and in computer systems that are connected to systems located on the premises of a unit or a service of the Police or of the Gendarmerie, in compliance with rules governing search, as long as this data is accessible from the initial system[60].

Where it is established in advance that this data, accessible from or for the initial system, is stored in a computer system that is located outside the national territory, it is collected subject to conditions of access under applicable international commitments.[61] Collected data may be copied onto any support, and digital supports may be seized and placed under seals under the conditions set out by the Penal Procedure Code.[62]

The above-mentioned provision has the following implications:

- In case the judicial police officer is not aware that data is stored outside the national territory, he or she can search and copy it as if this data would be stored in France[63]. The police officer has moreover no obligation to locate data before accessing it.

[59] Article 57-1 PPC (relating to flagrancy investigations). See also (for the application of the same rules within the framework of preliminary investigations and judicial information) articles 76-3 and 97-1 PPC.
[60] Article 57-1, §2 PPC.
[61] Article 57-1, §3 PPC.
[62] Article 57-1, §4 PPC.
[63] Alexandre Rousselet-Magri, Les perquisitions « informatiques » à l'épreuve du principe de souveraineté, dans un contexte de mondialisation du stockage de données, Étude comparée en droit français et états-unien *("Electronic" searches facing the principle of sovereignty, within a context of data storage globalisation, Comparative review of the French and American legislations)*, Dalloz, *Revue de science criminelle et de droit pénal comparé*, 2017/4 N° 4, p. 659 - 676, ref. p. 663, available online at https://www.cairn.info/revue-de-science-criminelle-et-de-droit-penal-

- In case the judicial police officer is aware that data are stored outside the national territory, this officer will have to comply with international commitments if some do exist, but at the current time the French Court of Cassation considers that (1) the Convention of Budapest of the Council of Europe will be applicable only if it is established during proceedings that data are stored outside the French territory[64], knowing that this Convention is only applicable where data that is sought is publicly available or is accessed with the consent of the person who has authority on the computer system[65]. In the absence of other identified international commitment regulating this precise situation, the Court of Cassation[66] considers that data stored abroad and accessible from a system located in France may be accessed based on the magistrate's decision regulating the initial search, without requiring any additional authorisation and without requiring the application of the general procedure for judicial cooperation described in Articles 694 *et seq.* of the PPC[67]. This position of the French Court of Cassation is however disputed by certain legal authors[68].

***These considerations raise the issue of access to mailboxes, in case the electronic identifier is found during the search****. Before the establishment, in the PPC, of the procedural power to access a mailbox by the means of using an electronic identifier (see Question n°13), the French Court of cassation considered that messages that the content of a mailbox may be intercepted by procedures other than the one dedicated to*

---

compare-2017-4-page-659.htm and https://www.dalloz.fr/lien?famille=revues&dochype=RSC%2FCHRON%2F2018%2F0004.

[64] Court of Cassation, Criminal Chamber, 6 November 2013, n°12-87130, Bull. Crim. n°9 (Nov. 2013) n° 217, https://www.courdecassation.fr/IMG/pdf/bull_crim_1311.pdf, also available online at https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000028173585&fastReqId=18162556&fastPos=1. See also Alexandre Rousselet-Magri,, *op. cit.*, p. 665-666.

[65] Art. 32 of the Convention on cybercrime of the Council of Europe, adopted in Budapest on 23 November 2001, to which France is a Party.

[66] Court of Cassation, Criminal Chamber, 6 November 2013, n°12-87130, *op. cit.*; Court of Cassation, commercial chamber, 26 February 2013, n° 12-14772, https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000027127622&fastReqId=794519744&fastPos=1; See also Alexandre Rousselet-Magri,, *op. cit.*, p. 667.

[67] See the answer under question n° 13.

[68] Sophie Sontag Koenig, Les perquisition 2.0 : quand l'informatique se saisit de l'immatériel *(Searches 2.0 : where computing handles the intangible)*, AJ pénal 2016. 238, mentioned in Alexandre Rousselet-Magri, *op. cit.*, p. 664.

*correspondence interception, and particularly the search and seizure procedure.*[69] *Its decisions have mostly concerned seizures performed on the basis of article L. 450-4 of the Commerce Code, which provides for a specific search and seizure procedure that can be implemented by investigating services of the competition authority upon authorisation of the liberty and custody judge*[70]*. Within this framework, the Court of Cassation has also considered that the content of a mailbox is unbreakable*[71]*, and that, as a result, it may be globally seized as soon as it includes elements partly useful to prove alleged wrongdoing*[72]*. The Court of Cassation also ruled that the irregular seizure of certain files or documents (such as correspondence exchanged between an advocate and their client) has no effect on the validity of the operations of search and of the seizure of other materials*[73]*.*

*Moreover, in a decision of 8 July 2015*[74] *related to judicial investigations, the Court of Cassation made a clear distinction between emails received from the date of a written decision of correspondence interception taken by an investigating judge, which are subject to this very procedure, and emails "sent or received" before the date of this interception decision, which "collection, registration and transcription [...] must be*

---

[69] See for ex. Court of cassation, criminal chamber, 8 July 2015, n° 14-88457, bull., available at https://www.courdecassation.fr/jurisprudence_2/chambre_criminelle_578/3648_8_32306.html; Court of cassation, criminal chamber, 9 March 2016, n°14-84566 , bull., available at https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000032193829&fastReqId=1781896582&fastPos=1.

[70] Court of cassation, crim. ch., 9 March 2016, n°14-84566, bull., https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000032193829&fastReqId=1781896582&fastPos=1; Court of cassation, crim. ch., 23 November 2016, n°15-81131, https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000033483607; Court of cassation, crim. ch., 20 December 2017, n°16-83469, https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000036343934; Court of cassation, crim. ch., 4 May 2017, n°16-81062, https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000034653409&fastReqId=1731033929&fastPos=3.

[71] Court of cassation, crim. ch., 20 December 2017, op. cit.

[72] Court of cassation, crim. ch., 23 November 2016, op. cit.

[73] Court of cassation, crim. ch., 4 May 2017, op. cit.; Court of cassation, 20 December 2017, *op. cit.*

[74] Court of cassation, criminal chamber, 8 July 2015, n° 14-88457, bull., available at https://www.courdecassation.fr/jurisprudence_2/chambre_criminelle_578/3648_8_32306.html. . Previously, the Court of Cassation considered that the content of mailboxes could be seized: see for ex. Cour de cassation, ch. crim., 6 November 2013, n° 12-87130 (arrêt n° 5362), https://www.courdecassation.fr/jurisprudence_2/chambre_criminelle_578/5362_6_27718.html.

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

*performed in compliance with provisions regulating seizure"*[75]*, in particular where this correspondence has been "stored before the date" of this written decision*[76].

*No one of the above-mentioned decisions made a distinction between emails actually received by the recipient (and therefore opened by the recipient), emails technically received by the hosting provider but not opened by the recipient, and emails written by the owner of the mailbox but standing in an outbox or returned due to a delivery failure not yet known about by the mailbox owner. However, a legal analysis performed in accordance with the doctrinal definition of correspondence and the principles enshrined in the decisions of both the French Constitutional Council and the ECtHR leads to the conclusion that correspondence should be protected as soon as the sender has initiated the sending of his or her correspondence, until this correspondence has been received by the addressee as a person. During this timeframe, no correspondence should be accessed outside the procedure set-up for correspondence interception, whatever its medium of transmission and its medium of storage*[77].

*The position of the Court of Cassation is therefore questionable, since the search and seizure procedure does not provide for sufficient guarantees in relation to correspondence protection. As a result correspondence stored in a mailbox should not be intercepted using means other than the correspondence interception procedure or another procedure offering similar guarantees, if not higher. This principle should at least concern correspondence that is being sent and correspondence that has not been opened by the recipient person, and should by extension concern the entire contents of a mailbox, where there is no practical possibility to access voluntarily stored correspondence without having knowledge of correspondence that is still under transmission.*

*The sole advantage of the search and seizure procedure, compared to the interception procedure, is that it is in principle performed in the presence of the owner of the*

---

[75] Translated from French: "l'appréhension, l'enregistrement et la transcription de correspondances émises ou reçues par la voie des télécommunications antérieurement à la date de la décision écrite d'interception prise par le juge d'instruction […] doivent être réalisés conformément aux dispositions légales relatives aux perquisitions."
[76] Translated from French: "y compris celles stockées antérieurement à l'autorisation d'interception."
[77] For further developments see Estelle De Marco, Country report France, published in Ulrich Sieber / Nicolas von zur Mühlen (eds.), Access to Telecommunication Data in Criminal Justice - A Comparative Analysis of European Legal Orders, Max-Planck-Institut für auslandisches Strafrecht, Berlin, 2016, ISBN: 978-3-86113-796-2, available at: https://csl.mpg.de/en/publications/access-to-telecommunication-data-in-criminal-justice/. Update to be published in the course of 2020-2021.

*mailbox, whereas the interception procedure is secret*[78]*. However, this benefit remains theoretical since secret access to the content of emails may be admitted as an investigating act*[79]*, and since the decisions of the Court of Cassation relating to investigation in the cloud, even hosted outside the French territory, do not require the presence of the owner of the mailbox during search into it at a police premise (the owner assisting only to the search at his or her premise).*

In addition[80], the French Court of cassation ruled[81] that French investigators may require, from a service provider located outside the French territory, the delivery of information such as an address or electronic documents coming from a computer system or database, even covered by professional or correspondence secrecy. The Court considers that, as long as investigators do not use any coercive means within the framework of such a request, and that the foreign service provider is free to answering or not answering this request, this act must be analysed as a simple "document delivery", within the meaning of Article 77-1-1 PPC (and therefore 60-1 PPC), and not as a search within the meaning of Article 57-1 PPC. The Court of Cassation considers that such "document delivery" does not infringe neither international law rules

[78] See for ex. on this issue J.P. Karsenty & associés, *Recueillement de données électroniques : interception de correspondances ou perquisition ? [gathering of electronic data; correspondence interception or judicial search?]*, 2015, https://www.jpkarsenty.com/Recueillement-de-donnees.html.

[79] See for example a decision of the Court of Cassation which validates the use of a password in order for investigators to access a private electronic space within the framework of an investigation, such action not requiring a specific authorisation from the judge who ordered the search and seizure procedure that enabled the discovery of the password (this decision could be extended to mailboxes): Court of cassation, ch. crim., 6 November 2013, n°12-87130, 6° moyen [ground of appeal], https://www.courdecassation.fr/jurisprudence_2/chambre_criminelle_578/5362_6_27718.html; In addition, the Court of Cassation has validated the possibility for investigators to obtain copies of emails from Google located in USA on the basis of a non-binding requisition: Court of Cassation, same decision, 2° and 3° moyens [grounds of appeal], comment available at https://www.legalis.net/actualite/enquete-preliminaire-validation-de-requisitions-directes-de-donnees-aupres-de-google-inc/. Previously, the Court of Cassation considered that a request for the content of emails addressed to operators located in France was irregular, but was not a cause for nullity since no email had been transcripted (which is contestable since secrecy of correspondence may have been violated): Cour de cassation, crim. ch., 22 October 2013, https://www.legalis.net/jurisprudences/cour-de-cassation-chambre-criminelle-arret-du-22-octobre-2013/.

[80] This paragraph is also included under question n°28 since it relates to provisions mentioned under this latter question.

[81] Court of cassation, criminal chamber, 6 November 2013, n° 12-87130, second part (« deuxième moyen »), available at https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000028173585&fastReqId=18162556&fastPos=1.

(since there is no direct and positive act performed by investigators outside their territory), nor the right of defence since the documents obtained are submitted to the parties to the proceedings for discussion and to the discretion of the judges. As a result, the Court of Cassation does not consider such request as an abuse of process, and does not consider that nullity is incurred.

***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?*

The answer under question n° 25 is also applicable here.

***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?*

Some provisions of the PPC enable it:

- Arts. 706-95-1 to 706-95-3 PPC, which enable remote access to correspondence stored by means of electronic communication, accessible using an electronic identifier (see answer under question n°4 and the Appendix).

- Art. 57-1 PPC, 76-3 and 97-1 PPC[82], which enable investigators to search for computer data that is of interest for the investigation and that is stored in computer systems that are connected to systems located on the premises of a unit or a service of the Police or of the Gendarmerie, as long as this data is accessible from the initial system (see the answer under Question n°17, Question n°25 and the Appendix). These provisions enable to search in a remote information system where, for example, access codes have been found during a search. The Court of Cassation[83] considers that data stored abroad and accessible from a system

[82] Article 57-1 PPC relates to flagrancy investigations. Same rules are applicable to preliminary investigations and judicial information as stated in articles 76-3 and 97-1 PPC.
[83] Court of Cassation, Criminal Chamber, 6 November 2013, n°12-87130, *op. cit.*; Court of Cassation, commercial chamber, 26 February 2013, n° 12-14772,

located in France may be accessed based on the magistrate's decision regulating the initial search, without requiring any additional authorisation[84].

***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?*

Several provisions enable investigators to obtain data from services providers.

- Article 60-1 PPC[85] empowers the district prosecutor or the judicial police officer or, under the latter's supervision, the judicial police agent, to order any person, establishment or organisation, whether public or private, or any public services likely to possess any documents relevant to the inquiry in progress, including those produced from a computer system or a personal data processing system, to provide them with this information, in particular in digital form, where needed in compliance with norms established by regulation, Without legitimate grounds, the duty of professional secrecy may not be given as a reason for non-compliance. Where such orders relate to the persons mentioned in articles 56-1 to 56-5[86], the transfer of the information may only take place with their consent. With the exception of the persons mentioned in articles 56-1 to 56-5 PPC, the failure to respond to such an order as quickly as possible is punished by a fine of €3,570.

---

https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000027127622&fastReqId=794519744&fastPos=1; See also Alexandre Rousselet-Magri,, *op. cit.*, p. 667.

[84] See the answer under question n° 13.

[85] This translation corresponds to the update, made by the author of the current report, of the translation of the PPC proposed on the French legal portal "Legifrance" and dated from 2005, which is available at https://www.legifrance.gouv.fr/content/location/1741 from https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations.

[86] Articles 56-1 to 56-5 PPC organise special protection, respectively, for lawyers/barristers, for press enterprises and journalists, for medical doctors, for notaries and bailiffs, in places identified as hosting information covered by national security, and for Courts facility and home of persons who exercise judicial functions where the search aims at seizing documents that are likely to be covered by deliberation secrecy. See Appendix, search and seizure, Art. 56 PPC.

Under pain of nullity, cannot be included in the case file an information gathered based on an order taken in violation of Article 2 of Law of 29 July 1881 on press freedom[87].

The above-mentioned provision is applicable to flagrancy investigations. The PPC provides for similar provisions within the framework of preliminary investigation[88] and judicial information[89].

In addition, the French Court of Cassation ruled[90] that French investigators may require, from a service provider located outside the French territory, the delivery of information such as an address or electronic documents coming from a computer system or database, even covered by professional or correspondence secrecy. The Court of Cassation considers that, as soon as investigators do not use any coercive means within the framework of such a request, and that the foreign service provider is free to answering or not answering this request, this act must be analysed as a simple "document delivery", within the meaning of Article 77-1-1 PPC (and therefore 60-1 PPC), and not as a Search within the meaning of Article 57-1 PPC. The Court of Cassation considers that such "document delivery" does not infringe neither international law rules (since there is no direct and positive act performed by investigators outside their territory), nor the right of defence since the documents obtained are submitted to the parties to the proceedings for discussion and to the discretion of the judges. As a result, the Court of Cassation does not consider such request as an abuse of process, and does not consider that nullity is incurred.

[87] Article 2 of Law of 29 July 1881 protects journalists' sources.
[88] Article 77-1-1 PPC.
[89] Article 99-3 PPC.
[90] Court of cassation, criminal chamber, 6 November 2013, n° 12-87130, second part (« deuxième moyen »), available at https://www.legifrance.gouv.fr/affichJuriJudi.do?oldAction=rechJuriJudi&idTexte=JURITEXT000028173585&fastReqId=18162556&fastPos=1.

- Article 60-2 PPC[91] empowers judicial police officers, or, under the supervision of the latter, of the judicial police agents, intervening by means of telecommunications or computers, to require from public organisations or private legal persons, with the exception of those set out in paragraph 2 d of Article 9 of the EU Regulation 2016/679 of 27 April 2016 and in paragraph 2 of Article 80 of Law no. 78-17 of 6 January 1978 relating to computers, files and liberties[92], to make available information helpful for the discovery of the truth, with the exception of information the secrecy of which is protected by law, where it is stored in one or more computer or personal data processing systems that they administer.

  According to the same article, these same investigators, intervening on the orders of the district prosecutor authorised in advance by a decree from the liberty and custody judge, may require telecommunications operators to take without delay all appropriate measures to ensure the preservation, for a period that may not exceed one year, of the text of the information consulted by persons using the services provided by the operators.

  Article 60-2 also states that the organisations or persons to which this article applies must make the required information available as quickly as possible by telematic or electronic means. Refusal to respond to such a request without a legitimate reason is punished by a fine of €3,750. A Decree of the Conseil d'Etat made on the advice of the National Commission for Data Protection determines the categories of organisation covered by the first paragraph, and also the methods for examining, transmitting and processing the required information.

[91] This translation corresponds to the update, made by the author of the current report, of the translation of the PPC proposed on the French legal portal "Legifrance" and dated from 2005, which was available until recently at https://www.legifrance.gouv.fr/content/location/1741 from https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations.

[92] Article 80 §2 refers to journalists exercising as professionals.

Article 60-2 PPC is applicable to flagrancy investigations. However the PPC provides for similar provisions within the framework of preliminary investigation[93] and judicial information[94].

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

No.

***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.*

No. Some requirements are provided for under the pain of nullity (see the answer under Question n°17 and the Appendix). In other situations, see the answer under Question n°15, which is also applicable to evidence collected during search and seizure.

*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.*

[93] Article 77-1-2 PPC.
[94] Article 99-4 PPC.

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

**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.*

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

Investigators intervening on electronic evidence have generally been trained. The Gendarmerie and the National Police have both a department composed of investigators who are specialised in such investigations. In addition, the Ministry of Justice and the Ministry of Interior issued guidelines available to investigators, recalling inter alia the steps to be followed in order to ensure that the seal (which most of the time will be sealed on the searched place) presents the necessary qualities (such as authenticity and integrity). However, there is no obligation for an investigator to ask for the assistance of skilled colleague, which may lead to inquiries or examinations that do not follow the state of the art.

This being said, during the analysis, investigators must document steps that have been followed in order to avoid the evidence being challenged by the defense. Indeed, other parties may raise the issue of the integrity, relevance or authenticity of the evidence in case the analysis steps cannot be demonstrated or if they did not follow appropriate rules.

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

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

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

No rules other than those set-up in Articles 230-1 *et seq*. (see the answer under Question n°6) regulate mobile forensics tools using/deploying AI technology. Without more detailed precisions, I do not see what could prevent such use, under the reserve that the fairness of proceedings and the rights of the defense are preserved (including the possibility to challenge the undisputable nature of results obtained using AI technology). Must also be respected the data protection prohibition of decisions based solely on automated processing which produce adverse legal effects concerning the data subject (Article 11 of Directive 2016/680).

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

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

Rules of judicial cooperation do apply (see the answers under Questions n°13, 17 and 25).

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

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

Once there is a need for judicial cooperation (which means where the investigation must be performed outside the French territory and that powers developed under Questions n°17 an n°25 do not apply), rules for judicial cooperation apply (see the answer under Question n°13 in relation to their content).

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

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

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

The practice is to follow Arts. 694 *et seq.* of the PPC in the absence of any international convention or bilateral treaty stipulating otherwise[95]. As explained in the answer to Question n°13, a first chapter dedicated to general provisions regulates the transfer and execution of judicial assistance requests (articles 694 to 694-4-1), assistance for the purpose of hearing, surveillance and infiltration (articles 694-5 to 694-9), and judicial assistance for the purpose of seizure of the proceeds of penal infringements with a view to subsequent confiscation (articles 694-10 to 694-13).

A second chapter dedicated to the provisions that are specific to judicial assistance between France and the other EU member States regulates European investigation orders (articles 694-15 to 694-50), joint investigation teams (articles 695-2 to 695-3), the EUROJUST unit (articles 695-4 to 695-7), the EUROJUST national representative (articles 695-8 and 695-9), the issue and execution of orders freezing property or evidence (articles 695-9-1 to 695-9-30), simplified exchange of information between services in application of the framework decision of the EU Council of 18 December 2006 (articles 695-9-31 to 695-9-49), cooperation between Asset Recovery Offices of Member States in the area of tracing and identifying proceeds of crimes and other goods in relation to crime, in application of Decision 2008/845/JHA of the Council of 6 December 20017 (articles 695-9-50 to 695-9-53), and the prevention and resolution of conflicts of competence exercised in application of the framework decision of the Council of the European Union of 30 November 2009 (articles 695-9-54 to 695-9-57).

A third Chapter contains one provision pertaining to judicial assistance between France and certain States (article 695-10).

[95] Art. 694 PPC.

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

A fourth Chapter contains provisions regulating the European arrest warrant, procedures for transfer between Member States resulting from the EU Council framework decision of 13 June 2002 and procedures for transfer resulting from agreements concluded by the European Union and other States (articles 695-11 to 695-58).

In addition, France has ratified the Council of Europe Convention on cybercrime with two reservations in relation to its content.

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

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

Cooperation rules are established within the respect of the PPC. Some cooperation practices with the foreign private sectors do also exist as illustrated in the answer to Question n°28.

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

## 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.

Previous answers did already widely answer this question.

-The Data protection Directive, which has been transposed under French law, must be respected.

-The PPC establishes rules that preserve the right to defense and the proportionality of the seizure. Inter alia:

-The preliminary Article to the PPC states that during the course of the penal procedure, measures that invade the privacy of a person may only be taken, upon decision and under the effective supervision of the judicial authority, where they are necessary to establish the truth and proportionate to the severity of the offence, taking into account factual circumstances.

- Art. 56 PPC states the following:

*(The judicial police officer) is the only person, together with those persons mentioned under article 57 and any persons upon whom he calls pursuant to article 60, to be allowed to examine the papers or documents or computer data before proceeding to seize them.*

*However, without prejudice to the application of Articles 56-1 à 56-5*[96]*, he has the duty first to initiate any step appropriate to ensure the observance of professional secrecy and of the defendant's rights.*

*Any article or document seized is immediately entered on an inventory and placed under official seals. However, if itis difficult to make such an inventory on the spot, they are put under temporary closed official seals until such time as an inventory can be taken and they can be placed under final official seals. This is done in the presence of the persons who have witnessed the search pursuant to the conditions set out by article 57.*

*The seizure of any computer data necessary for the discovery of the truth is carried out by placing in the hands of justice, either the physical medium holding this data or a copy of the data made in the presence of those persons present at the seizure.*

*(…).*

*With the agreement of the district prosecutor, the judicial police officer only allows the seizure of objects, documents or computer data useful for the discovery of the truth, (…).*

-Rights to a fair trial and to non-discrimination are applicable, and the defense of the accused may always challenge evidences presented by investigators.

-All information that is useful to discover the truth might be copied. The time during which it can be kept is regulated by the PPC depending on the procedure that is followed and the power that is

[96] Articles 56-1 to 56-5 PPC organise special protection, respectively, for lawyers/barristers (a search at their home or office can only be carried out by a magistrate in the presence of the Bar President or his delegate and pursuant a written and reasoned decision taken by this magistrate, the magistrate and the Bar President are the solely persons who can consult documents before their seizure and the seizure cannot include documents or objects that relate to other infringements that are not mentioned in the above-mentioned decision – all these requirements being decreed under penalty of nullity; the Bar President or his delegate may oppose the seizure of a document or of an object, which will be settled by the liberty and custody judge), for press enterprises and journalists (a search at their home or office and cars can only be carried out by a magistrate, other rules being *mutatis mutandis* the same as those concerning lawyers), for medical doctors, notaries and bailiffs (a search at their office can only be carried out by a magistrate in the presence of the person responsible for the order or professional organisation to which the person concerned belongs, or its representative – Art. 56-3 PPC does not include any other derogations); in places identified as hosting information covered by national security (search can only be carried out by a magistrate in the presence of the President of the Commission of national security secrecy, other rules being mostly, *mutatis mutandis*, the same as those concerning lawyers), and for Courts facility and home of persons who exercise judicial functions where the search aims at seizing documents that are likely to be covered by deliberation secrecy (search can only be carried out by a magistrate in the presence of the First President of the Court of Appeal or the First President of the Court of Cassation or its delegate, other rules being mostly, *mutatis mutandis*, the same as those concerning lawyers).

used, but stays unclear in relation to the seizure and copy after seizure of electronic evidence. Article 41-4 PPC states that six months from the day of the decision disposing of the matter, or from the decision by which the last court seized has extinguished its jurisdiction, the unreturned articles become the property of the State, subject to the rights of third parties. The district prosecutor may decide to destroy these articles or not. Some specific procedures authorise a longer retention in important matters.

Special rules are also established in relation to data collected remotely (*inter alia* for the powers evoked in the first part of the current report, non-related to Search and seizure), which are hosted in a National platform for interception, and which obey to particular rules in relation to data suppression.

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

## Section 3: Admissibility of evidence before court

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

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

No.

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

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

Yes. The importance is to preserve the authenticity of the evidence, its integrity, and to be able to demonstrate that conclusions are liable, in order to avoid the evidence to be challenged before the judge.

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

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

Yes, this topic has already been developed under Question n°15. The judge will pronounce the nullity where this penalty is prescribed by the PPC, and in other case he or she will rule on the admissibility and probative value of the evidence, upon request of the interested party.

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

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

If it has been accessed based on an initial search decision, the Court of Cassation considers that it is an act of procedure that does not need any other legal basis (see the answer under Question n°25). This same courts also consider that French investigators may require, from a service provider located outside the French territory, the delivery of information such as an address or electronic documents coming from a computer system or database, even covered by professional or correspondence secrecy, as long as investigators do not use any coercive means within the framework of that request, and that the foreign service provider is free to answering or not answering this request (see the answer under Question n°25).

In other cases and where the Budapest Convention of the Council of Europe is not applicable (where data are not publicly available or where data were accessed with the consent of the person who has authority on the computer system), the general procedure for judicial cooperation described in Articles 694 et seq. of the PPC should have been followed and the judge may pronounce the nullity of acts carried-on without being frame by the latter.

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

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

The judge will be the one to decide on the admissibility of evidence and its probative value. See the answer under Question n°15.

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

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

Not beyond answers already brought previously in the current report.

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

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

Jurisprudence has been briefly presented under Question n°15. Other court decisions are on the same line.

For example, the Court of Cassation[97] admitted the use of an evidence found on a computer data storage medium by a qualified person, whereas this storage medium had not been placed under seal, since there was no doubt regarding the identity of the owner of the medium seized, since this owner was present during the seizure, and since this owner did not contest the data that has been extracted and transcribed in official reports. In this context, the Court of Cassation considered that interests of the accused person had not been affected.

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

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

No.

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

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

[97] Court of cassation, criminal chamber, 30 March 2016, n° 15-86693, https://www.legifrance.gouv.fr/affichJuriJudi.do?idTexte=JURITEXT000032350365.

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

It might be enough, provided that the interested party raises the issue.

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

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

Yes, I already provided examples of case law where such evidence was questioned. In such case, a decision of inadmissibility or of discard for absence of probative value is always possible (for instance if the interested party demonstrates an issue of integrity or of traceability).

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

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

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

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

In relation to the two first questions, answers have been brought previously in the current report, particularly under Question n°15.

Recourse to experts is possible, but they must either be registered on one of the lists provided for by article 157 PPC, or must called upon take an oath in writing to assist the administration of justice upon their honour and conscience[98].[99]

Otherwise, the forensic examination is conducted by the judicial police officer, who may be assisted by an agent of the judicial police having a qualification[100].

[98] Confirmed by the Court of cassation, criminal chamber, 21 June 2006, n° 06-82774.
[99] Articles 60, 77-1 and 81 PPC.
[100] Called ICC in the National Police and NTECH in the Gendarmerie.

The National Police[101] and the National gendarmerie[102] also welcome a special national unit that may be requested in order to carry on forensic examinations following the state of the art. In addition, qualified investigators are progressively deployed throughout the territory.

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

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

No.

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

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

There is no recognised standardization to be followed. However, there are guidelines corresponding to the state of the art and therefore considered as critical in order to ensure that courts will recognise the admissibility and probative value of evidence, through ensuring evidence authenticity, integrity, traceability, durability, usability and interpretation. These guidelines also recall the Penal Procedure Code requirements.

[101] See https://www.police-scientifique.com/scpts.
[102] See https://www.gendarmerie.interieur.gouv.fr/pjgn/ircgn/division-criminalistique-ingenierie-et-numerique-dcin/departement-informatique-electronique-inl and https://www.gendarmerie.interieur.gouv.fr/pjgn/pjgn/la-chaine-criminalistique.

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

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

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

I did not find any.

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

***51.* 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.

All evidences must be communicated to parties before the trial, as regulated by the PPC depending on the procedure that is followed, and can be challenged as regards their legality, admissibility and probative value. A set of rules also enables the accused person to know his or her rights, including his or her right to remain silent and to be assisted by a barrister. However, a part of the equality of rights still lies on the judges and barristers understanding of technologies and evidences' value.

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

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

No training is legally required, but curricula do exist in order to train investigators who are specialised in this matter. The spread of specialised investigators throughout the territory is an objective and is progressively implemented. The latter can afterward assist and train in turn their colleagues. Training for magistrates are also organised by the Magistracy National School. Barrister cannot advertise on their specialisation without having followed a particular procedure organised by the Bar. Court experts are not trained but they must, in order to get this qualification and be registered on the list of a Court of appeal, prove their knowledge through the production of a CV and some works already performed in the area in which they want to become recognise as experts. However, in practice, the rigour and relevance of some court experts reports is controversial.

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

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

Flagrancy inquiries are limited to eight days and, where the offence is punishable by at least 5 years of imprisonment, this period might be extended for a further period of eight days[103]. The term of preliminary inquiries is not regulated but judges may have to pronounce themselves on its acceptable nature.

At the end of the inquiry, the district prosecutor decides to either close the case, or to initiate a legal proceedings (which might consist in the opening of a judicial information, mandatory in case of felony, which is limited to six, eight, ten or twelve months depending on the nature of the offence), or to choose in some case alternatives procedures where the PPC allows it. The time limit for proceedings is, from the offence or its establishment, 10 years for felonies and 3 years for misdemeanours. This time limit is interrupted by any act of inquiry or prosecution.

Within this framework, there is no particular time-limit obligation in relation to forensic examination.

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

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

**Globally,** the preliminary Article of the PPC[104] states that criminal procedure should be fair and adversarial and preserve a balance between the rights of the parties. It should guarantee a

[103] Article 53 PPC.
[104] The following translations, in this answer to Question n°54, correspond to the update, made by the author of the current report, of the translation of the PPC that was proposed until recently on the French legal portal "Legifrance" and dated from 2005, at https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations.

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

separation between those authorities responsible for prosecuting and those responsible for judging. Persons who find themselves in a similar situation and prosecuted for the same offences should be judged according to the same rules. Part II of this preliminary Article states that the judicial authority ensures that victims are informed and that their rights are respected throughout any criminal process. Part III of this same Article states that every person suspected or prosecuted is presumed innocent as long as his or her guilt has not been established. Attacks on his or her presumption of innocence are proscribed, compensated and punished in the circumstances laid down by law. He or she has the right to be informed of charges brought against him or her and to be legally defended. Where the suspected or prosecuted person does not understand French, he or she has the right to be assisted by a translator in the language he or she understands, until the end of the proceeding, including during interviews with his or her barrister where these interviews have a direct link with an interrogation or a hearing. He or she has also the right, unless he or she specifically refuses it after having been fully informed, to obtain a translation of main materials of the case file that are essential to his or her defense and to guarantee the fairness of the trial. The coercive measures to which such a person may be subjected are taken by or under the effective control of judicial authority. They should be strictly limited to the needs of the proceedings, proportionate to the gravity of the offence charged and not such as to infringe human dignity. The accusation to which such a person is subjected should be brought to final judgment within a reasonable time. During the course of the penal procedure, measures that invade the privacy of a person may only be taken, upon decision and under the effective supervision of the judicial authority, where they are necessary to establish the truth and proportionate to the severity of the offence, taking into account factual circumstances. Every convicted person has the right to have his conviction examined by a second tribunal. Within the framework of proceedings for a felony or a misdemeanour, no verdict against a person shall be solely based on confessions he or she has made where prior to this confessions he or she has not been enabled to consult with his or her barrister and to be assisted by the latter.

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

**Within the framework of his or her duty to head the judicial police, the district prosecutor** may address general or specific instructions to investigators. He or she supervises the legality of the means that are implemented by the latter, the proportionality of investigative operations taking into account the nature and the severity of facts, as well as the orientation and quality of investigations.[105] The district prosecutor receives complaints and denunciations and decides how to deal with them, in accordance with the provisions of article 40-1. Every constituted authority, every public officer or civil servant who, in the performance of his duties, has gained knowledge of the existence of a felony or of a misdemeanour is obliged to notify forthwith the district prosecutor of the offence and to transmit to this prosecutor any relevant information, official reports or document.[106] Where he or she considers that facts brought to his or her attention in accordance with the provisions of article 40 constitute an offence committed by a person whose identity and domicile are known, and for which there is no legal provision blocking the implementation of a public prosecution, the district prosecutor with territorial jurisdiction decides if it is appropriate: (1) to initiate a prosecution; (2) or to implement alternative proceedings to a prosecution, in accordance with the provisions of articles 41-1 or 41-2; (3) or to close the case without taking any further action, where the particular circumstances linked to the commission of the offence justify this. [107] The public prosecutor informs victims about his or her decision [108] and any person who has reported an offence to the district prosecutor may lodge an appeal with the Attorney general if, following the prosecutor's report, the decision is taken to close the case without taking further action. The Attorney general may, under the conditions provided for by

[105] Article 39-3 PPC. This translation is based on the translation of the PPC proposed until recently on the French legal portal "Legifrance" at https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations.
[106] Article 40 PPC. This translation is based on the translation of the PPC proposed until recently on the French legal portal "Legifrance" at https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations.
[107] Article 40-1 PPC. This translation is based on the translation of the PPC proposed until recently on the French legal portal "Legifrance" at https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations.
[108] Article 40-2 PPC.

article 36, instruct the district prosecutor to initiate a prosecution. If he or she feels that the appeal is unfounded, he or she informs the party concerned of this. [109]

The district prosecutor institutes or causes to be taken any step necessary for the discovery and prosecution of violations of the criminal law. To this end, he directs the activity of the judicial police officers and agents within the area of jurisdiction of his court. He or she may also directly require any judicial police officer, on the whole national territory, to carry-up investigative actions that need to be executed outside his or her jurisdiction. He or she may himself or herself travel throughout the whole territory. [110]

Finally, the principle of fairness of the proceedings and the adversarial principle implies that evidence and other proceeding documents are communicated to the other party before the trial, spontaneously and in good time[111].

**Principles governing Courts** are in some aspects different depending on the nature of the legal text that bases proceedings (civil or penal) and of the offence (felony, misdemeanour or contravention).

As regards misdemeanours, offences may be proved by any mode of evidence except where the law otherwise provides. The judge decides according to his innermost conviction and he or she may base his decision solely on evidence that was submitted in the course of the hearing and adversarially discussed before him.[112] Confessions, as any other type of evidence, are left to the

[109] Article 40-3 PPC. This translation is based on the translation of the PPC (updated where necessary), proposed until recently on the French legal portal "Legifrance" at https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations.
[110] Article 41 PPC. This translation is based on the translation of the PPC (updated where necessary), proposed until recently on the French legal portal "Legifrance" at https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations.
[111] Principles of civil procedure that are also in use within the framework of penal proceedings and belong to the barristers' deontology. See for example Alain Provansal, Communication de pièces et office du Juge, 3 May 2013, https://www.eurojuris.fr/categories/procedure-penale-procedure-civile-7000/articles/communication-de-pieces-et-office-du-juge-1102.htm.
[112] Article 427 PPC

free appreciation of the judges.[113] Any official record or report has probative value only if it is formally regular, and if its drafter acted in the performance of his duties and reported what he personally saw, heard or found on a subject-matter within his jurisdiction. Every official record of an interrogation or a hearing must contain the questions which were answered therein. [114]

Except where the law provides otherwise, official records and reports establishing the existence of misdemeanours only have the value of simple information.[115] In the cases where judicial police officers, judicial police agents or the civil servants and agents entrusted with certain judicial police duties have been granted by a special legislative provision the power to establish misdemeanours by official records or reports, proof of the contrary may only be brought in writing or through witnesses.[116] If the court considers an expert report necessary, proceedings follow as stated under articles 156 to 166, 168 and 169.[117] The presiding judge interrogates the defendant and hears his statement before hearing the witnesses.[118]

Subject to the provisions of article 401, the public prosecutor and the advocates for the parties may put questions directly to the defendant, the civil party, the witnesses or anyone else called to testify, by asking the presiding judge for leave to speak. The defendant and the civil party may equally put questions through the presiding judge as intermediary.[119]

**The accused person** is informed about his or her rights whatever the means used to bring him or her into court (amongst the four means described in Article 388 PPC). He or she may, together with his or her barrister, require at any time during the trial an additional act that they consider necessary to establish the truth. [120]

[113] Article 428 PPC
[114] Article 429 PPC
[115] Article 430 PPC
[116] Article 431 PPC
[117] Article 434 PPC
[118] Article 442 PPC
[119] Article 442-1 PPC
[120] Article 388-5 PPC

At their request, the parties or their barrister may obtain a copy of the case file materials, which may be digital if the case file has been digitalised, subject to conditions established in Article 803-1 PPC. Delivery of this copy must happen within the month that follows the request (or two months in a particular case described in the PPC, in which the defendant may ask for a postponement of the trial if the latter begins before he or she obtained a copy of the case file – postponement which the judge must order[121]) and the first copy of each case file material is free of charge[122].

An alternative procedure of "immediate appearance", in which delays are reduced, may also be followed under certain conditions[123]. Where the defendant is brought into court following this procedure, the judge must inform him or her that he or she can be tried this very day at the condition he or she agrees and such agreement can only be given in the presence of his or her barrister[124].

**The victim** is a party to the trial only if he or she brings a civil action for the reparation of the damage suffered because of the felony, misdemeanour or petty offence. The civil action is open to all those who have personally suffered damage directly caused by the offence. The waiver of a civil action will not interrupt or suspend the exercise of the public prosecution, subject to exceptions established by law.[125] Victims are informed about their right, including the one to join a civil proceeding before the criminal court[126] and, as soon as possible, victims are subject to an individualised assessment in order to identify if they need specific protective measures during

[121] Article 390-2 PPC
[122] Article 388-4 PPC
[123] Article 395 PPC
[124] Article 397 PPC
[125] Article 2 PPC
[126] Article 10-2 PPC

penal proceedings[127]. Where the victim of a misdemeanour has lodged a complaint, he or she is informed by the prosecution office of the date of the hearing. [128]

**As regards witnesses**, any person summoned to be heard as a witness is obliged to appear, to take an oath and to make a statement[129]. However journalists have the right to not reveal their sources[130] and member of the family listed in the PPC, in addition to the civil party and children before 16 years old, witness without taking an oath[131].

## 5.1 The Prosecution

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

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

There is no particular guidance beyond what has already been exposed above.

## 5.2 The Court

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

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

Yes it may, on his or her own initiative where the PPC sets up requirements under the penalty of nullity (for example, all the provisions set up in Articles 56 and 57 are prescribed under the

[127] Article 10-5 PPC
[128] Articles 391, 393-1 and 397-1-1 PPC
[129] Articles 391, 393-1 and 397-1-1 PPC
[130] Articles 391, 393-1 and 397-1-1 PPC
[131] Articles 391, 393-1 and 397-1-1 PPC

penalty of nullity[132]), or upon request of the interested party in the other situations. Examples have been provided under Question n° 15.

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

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

There are no particular guidelines on the way to assess such evidence, unless the judge in charge has been trained to this. However judges may have recourse to judicial/courts experts.

## 5.3 The defendant and defender

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

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

This question has been answered under Question 54 as regards the access to the case file. The defendant and his or her barrister may challenge the evidence through explaining to the court that the followed methodology is not produced (which does not allow assessing the evidence's probative value) or does not guarantee the authenticity, integrity or reliability of the evidence or of its outcomes after forensic research.

[132] Article 447, 448 and 335 PPC.

## 5.4 Witnesses

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

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

Answer to this question has been partly brought under Question n° 54. For the rest, on the request of the president of the Court, the witnesses must state their surnames, first names, age, profession and domicile or residence, (only before the Assize Court: whether they knew the accused before the events mentioned in the referring judgment), whether they are family members or relations by marriage to either the accused or the civil party, and whether they serve one of them.[133] Before beginning their statements, the witnesses take an oath "(only before the Assize Court: to speak without hatred or fear, and) to tell the whole truth and nothing but the truth". Before the Assize Court, witnesses are to testify only in respect of the matters alleged against the accused, or in respect of his personality and his morality[134].

There are no 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. On these matters, technical judicial experts may be asked to analyse evidences and to witness about the outcomes of their analysis, by all parties.

## 5.5 The Victim

***60.*** **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*

[133] Articles 331 and 445 PPC.
[134] Article 331 PPC.

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

*obtained via mobile forensics when exercising their rights? Please refer to case law if possible.*

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

Beyond the answer brought to Question n°54, there are no particular other privacy preserving measures. Since they are party to the trial, they may use all the evidence produced in order to exercise their rights.

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

## Section 6: Comments

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

**Answer:** I answered this questionnaire in relation to penal procedure. Please also note that intelligence services in charge of the pursuit of a series of objectives including organised crime prevention, have also some interception powers.

Some findings coming from these services may be used in certain proceedings. In this case, they are not considered as evidence but as a simple information[135].

1. General observations including possible links with penal procedure

The following provisions may be used within the framework of the search for information by intelligence services and agents of several ministries listed by law and their implementing administrative acts, in the pursuit of a limited number of objectives.

These objectives are the search for information relating to the defence and promotion of the following "fundamental interests of the nation"[136]:

1) National independence, territorial integrity, and national defence;

2) Major interests of foreign policy, implementation of France's European and International commitments, and prevention of any form of foreign interference;

3) Major economic, industrial, and scientific interests of France;

4) Prevention of terrorism;

[135] César Ghrénassia et Robin Binsard, La preuve, le renseignement et le droit (Evidence, intelligence and Law), 3 June 2020, Dalloz actualité, https://www.dalloz-actualite.fr/node/preuve-renseignement-et-droit.
[136] According to the new art. L. 811-3 ISC, created by Law n° 2015-912 of 24 July 2015 of 26 July 2015.

5) Prevention of:

– a) attacks against the republican form of French institutions,

– b) actions pursuing the reconstitution or the preservation of disbanded groups,

– c) collective violence likely to cause serious harm to public peace;

6) Prevention of organised crime and delinquency;

7) Prevention of proliferation of weapons for mass destruction.

Theoretically, the aforementioned objectives are the only ones that can justify the exercise of the exceptional measures described in the Internal Security Code. However, a French legal provision and a Court of Cassation's decision both give rise to the possibility of using the information gathered within the framework of these powers in order to feed the investigation into any penal infringement.,

Indeed, the French Internal Security Code and Penal procedure Code law requires that any (other) crime or misdemeanour discovered upon exercising these special powers is brought to the attention of the public district prosecutor (who has the discretion to take action on it), accompanied by related information.

In addition, the French Court of Cassation decided, in a decision of 9 January 2018[137], that a Judicial Police officer, acting under articles 53 to 67 of the Penal Procedure Code that regulates flagrancy investigations, has the duty to ensure the preservation of evidence that will likely disappear and of all that can be used to ascertain the truth, and that this duty may justify the access of this police officer to data collected within another framework, including under administrative law (in this case were the data in issue was surveillance images collected upon authorisation of the prefect on the basis of the Internal Security Code). As a result, the access of

[137] Court of cassation, criminal chamber, 9 January 2018, n° 17-82.946 https://www.dalloz-avocats.fr/documentation/Document?id=CASS_LIEUVIDE_2018-01-09_1782946.

justice to data collected for State security reasons, within the framework of penal investigations and at the initiative of judicial investigators, is not excluded.

2. Administrative powers of interception

Electronic correspondence transmitted by means of electronic communications may be intercepted under article L. 852-1, I of the Internal Security Code. The interception can be extended beyond the concerned person, to the persons belonging to the environment of the latter where there are reasons to believe that these persons are likely to provide information connected with the purpose that justified the authorisation.

Electronic correspondence sent or received by terminal equipment may also be intercepted directly by means of a technical device or apparatus, in order to pursue certain purposes only[138], under article L. 852-1, II of the Internal Security Code.

Electronic correspondence transmitted within an electronic communication network using exclusively over-the-air transmission and not involving any electronic communication operator, may be intercepted in situation where this network is conceived to be domestically used by one person or a closed group of users, under article L. 852-2 of the Internal Security Code.

Traffic and connection data[139] retained by service providers[140] can be accessed according to articles L. 851-1 and L. 851-2 of the new Internal Security Code. Such access may be obtained

[138] Mentioned in 1°, 4° and 5° of article L. 811-3 ISC.

[139] More precisely, data that may be accessed is more widely identified by law (in art. L. 851-1, former art. L. 246-1) as being "*information or documents processed or stored* by (ISP's) networks or electronic communications services, including technical information relating to the identification of subscription or connection numbers to electronic communications services, to the census of all subscription numbers and connection numbers of a specified person, to the geolocation of terminal equipment used, and to a user's communications regarding the list of called and calling numbers, the duration and date of communications." The decree of application of the original provision (art. L. 246-1, created by Law n°2013-1168 of 18 Dec. 2013, art. 20), specified that this data is only that which is of a technical nature and cannot relate to the content of communications that can be accessed by the judiciary for the repression of crimes (Decree n°2014-1576 of 24 Dec. 2014 – http://www.legifrance.gouv.fr/eli/decret/2014/12/24/PRMD1422750D/jo). The decree of application of the new law (Decree n° 2016-67 of 29 Jan. 2016) refers to the same data. It provides for an additional list of data that may be accessed by intelligence services or other Ministries, but only within the framework of administrative correspondence intercepts. It should be noted that the

from these providers, or, solely for the purpose of terrorism prevention, through "real-time transmission"), concerning persons previously identified as being "likely to be linked to a threat" and persons belonging to the latter's environment where serious reasons suggest that they are likely to provide information linked to the purpose that justifies the authorisation of the measure.

Direct collection of some of this data (connection data of a technical nature enabling the identification of terminal equipment or the identification of the subscription number of its user, as well as location data of terminal equipment) by means of an intrusion into the computer system is organised by article L. 851-6 of the Internal Security Code.

Real-time geolocation of a person, a vehicle or an object, without the consent of the person or the owner of the vehicle or object, is provided for in articles L. 851-5 and L. 853-3 of the Internal Security Code.

In addition, technical data relating to the location of terminal equipments may be collected "by network solicitation" and transmitted "in real time" by electronic communication operators to a service of the Prime Minister, under article L. 851-4 of the Internal Security Code.

Computer data, as it is stored or as it is displayed on the screen of the user or typed or received or sent, may be captured remotely where intelligence cannot be collected by another legal means, under articles L. 853-2 and L. 853-3 of the Internal Security Code.

Words spoken in a private place or under confidentiality and images in a private place may be captured, where intelligence cannot be collected by another legal means, using a dedicated technical device, under articles L. 853-1 and L. 853-3 of the Internal Security Code.

---

French Constitutional Council has recalled that traffic data that can be accessed for intelligence purposes cannot be related to the content of correspondence or to consulted information (Decision n°2015-713 DC, recital n° 55, http://www.conseil-constitutionnel.fr/conseil-constitutionnel/root/bank/download/cc2015713dc.pdf – press release: http://www.conseil-constitutionnel.fr/conseil-constitutionnel/francais/les-decisions/acces-par-date/decisions-depuis-1959/2015/2015-713-dc/communique-de-presse.144139.html).

[140] This data is retained on the basis of art. L. 34-1 PECC (relating to electronic communications operators and access providers) and of art. 6 of the Law n°2004-575 of 21 June 2004 regarding confidence in the digital economy, so-called LCEN (relating to access and hosting providers).

International electronic communications, which means communications that are sent or received from abroad, may also be intercepted and are exclusively regulated by articles L. 854-1 to L.854-9 of the Internal Security Code, whatever they are related to correspondence or connection data.

Finally, all communications may be monitored at the service provider level, for the needs of the prevention of terrorist acts only, in order to detect "connections that may reveal a terrorist threat" under article L. 851-3 of the Internal Security Code.

## Appendix

**French Penal Procedure Code**

The translations proposed in the current report and the current Appendix correspond to the update, made by the author of the current report, of the translation of the PPC that was proposed until recently on the French legal portal "Legifrance" and dated from 2005[141]:

### PPC - Book IV: On some particular procedures

**Titre XXV: Procedure applicable to organised crime and delinquency and to crimes[142]**

**Chapter II – Procedure**

**Section 5 – Remote access to correspondence stored by means of electronic communication, accessible using an electronic identifier**

**Article 706-95** (modified by Ordonnance n°2019-964 of 18 September 2019)**:**

[141] Until recently available at https://www.legifrance.gouv.fr/Traductions/en-English/Legifrance-translations.
[142] From Article 706-73 of the Penal Procedure Code.

If the needs of a flagrancy inquiry or a preliminary inquiry into one of the offences within the scope of articles 706-73 and 706-73-1 justify this, the liberty and custody judge of the district court may, at the request of the district prosecutor, authorise the interception, the recording and the transcription of correspondence sent by electronic communication, under the provisions of paragraph two of article 100, article 100-1 and articles 100-3 to 100-7, for a maximum period of one month, renewable once under the same conditions of form and duration. These operations are carried out under the supervision of the liberty and custody judge.

The provisions of Article 100-8 are applicable to interceptions ordered under the current Article.

For the application of the provisions of articles 100-3 to 100-5 and 100-8, the powers conferred on the investigating judge or the judicial police officer appointed by him are exercised by the district prosecutor or the judicial police officer required by this magistrate.

The liberty and custody judge who authorised this interception is informed without undue delay by the district prosecutor of any actions carried out in accordance with the previous paragraph, including official records drawn-up pursuant to his authorisation, by way of the application of articles 100-4 and 100-5.

**Article 706-95-1** (modified by Law n°2019-222 of 23 March 2019)**:**

If the needs of an inquiry into a crime or into one of the offences within the scope of articles 706-73 and 706-73-1 justify this, the liberty and custody judge of the district court may, at the request of the district prosecutor, authorise, by way of reasoned order, access, remotely and without the knowledge of the person concerned, to correspondence stored by means of electronic communication and accessible using an electronic identifier. Data to which access has been enabled can be seized and registered or copied on any support.

**Article 706-95-2** (modified by Law n°2019-222 of 23 March 2019)**:**

If the needs of a judicial information into a crime or into one of the offences within the scope of articles 706-73 and 706-73-1 justify this, the investigating judge may authorise, by way of

reasoned order, access, remotely and without the knowledge of the person concerned, to correspondence stored by means of electronic communication and accessible using an electronic identifier. Data to which access has been enabled can be seized and registered or copied on any support.

**Article 706-95-3** (created by Law n°2019-222 of 23 March 2019)**:**

Operations mentioned in articles 706-95-1 and 706-95-2 are carried out under the authority and supervision of the magistrate who authorised them and cannot, under penalty of nullity, pursue another purpose than that of investigating and detecting penal infringements that are mentioned in the decision of this magistrate.

The magistrate or the judicial police officer appointed by him or her may require any qualified agent of a service, of a unit or of a body placed under the authority of the Minister in charge of electronic communication, or any qualified agent of an authorised network operator or provider of electronic communication services to set up the operations mentioned in the same articles 706-95-1 and 706-95-2.

The fact that these operations reveal penal infringements other than those mentioned in the magistrate's decision that authorises these operations is not a cause for nullity of incidental proceedings.

Where the electronic identifier is linked to the account of an advocate, of a magistrate, of a member of the Parliament or of a senator, article 100-7 is applicable.

## Book IV: On some particular procedures

## Titre XXV: Procedure applicable to organised crime and delinquency and to crimes[143]

## Chapter II – Procedure

[143] From Article 706-73 of the Penal Procedure Code.

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

## Section 6 – Other special investigation techniques

### §1 – General provisions[144]

**Article 706-95-11** (created by Law n°2019-222 of 23 March 2019[145])**:**

Provisions of the current paragraph are applicable to special investigative techniques mentioned in the current Section.

These special investigative techniques may be implemented if the needs of an inquiry or of a judicial information[146] into one of the penal infringements within the scope of articles 706-73 and 706-73-1 justify it.

**Article 706-95-12** (created by Law n°2019-222 of 23 March 2019)**:**

Special investigative techniques are authorised:

- During investigation, by the liberty and custody judge of the district court at the request of the district prosecutor;

- During a judicial information, by the investigative judge, after consultation with the district prosecutor.

**Article 706-95-13** (created by Law n°2019-222 of 23 March 2019)**:**

---

[144] Applicable to the collection of connexion technical data and interception of correspondence sent through electronic communication (Art. 706-95-20), to the collection of sounds and images in certain places and vehicles (Arts. 706-96 to 706-98) and to remote capture of computer data (Arts 706-102-1 to 706-102-5).
[145] Before this law and the creation of that section of the Code, (close) rules of procedures where described under the Section regulating each particular power.
[146] Law n° 2019-222 provided for that these special investigative techniques would also apply within the framework of any crime, but this adjunction has been considered unconstitutional by the Constitutional Council in its decision n° 2019-778 DC du 21 mars 2019. As a result, these techniques only apply within the framework of organised crime.

The authorisation referred to in Article 706-95-12 is given by way of written and reasoned order, referring to issues of fact and law that justify that these operations are necessary. It is not a decision of a judicial nature and it is not subject to appeal.

**Article 706-95-14** (created by Law n°2019-222 of 23 March 2019)**:**

These special investigative techniques are carried out under the authority and the supervision of the magistrate who authorised them. The latter may at all time order their interruption.

The liberty and custody judge is informed without undue delay by the district prosecutor about acts that have been accomplished. Official records that have been drawn-up pursuant to the implementation of the order of the liberty and custody judge are communicated to him or her.

If the liberty and custody judge considers that the operations were not carried out in compliance with his or her authorisation or that the applicable provisions of the current Code were not respected, he or she orders the destruction of official records that were drawn-up and of records that were made. He or she gives his or her decision by way of reasoned order that he or she notifies to the district prosecutor. The latter may lodge an appeal before the president of the Investigation Chamber within a period of time of ten days from the date of notification.

Under penalty of nullity, operations cannot pursue another purpose than that of investigating and detecting penal infringements that are mentioned in the decisions of this magistrate. The fact that these operations reveal penal infringements other than those mentioned in these decisions is not a cause for nullity of incidental proceedings.

**Article 706-95-15** (created by Law n°2019-222 of 23 March 2019)**:**

In case of emergency resulting from an imminent risk of evidence being damaged or an imminent risk of serious harm the rights of individuals or goods, the authorisation mentioned under Article 706-95-12 may be delivered as follows:

[1° removed from the law because it has been declared unconstitutional – decision 2019-778 DC of 21 March 2019]

2° In the course of a judicial information, by the investigative judge, without seeking a prior opinion from the district prosecutor.

The authorisation must be given in writing and reasoned. It includes the statement of factual circumstances that establish the imminent risk referred to in §1 of the current Article.

**Article 706-95-16** (created by Law n°2019-222 of 23 March 2019)**:**

The authorisation decision taken pursuant to §1 of article 706-95-12 is delivered for a maximum duration of one month, renewable once under the same conditions of form and length.

The authorisation decision taken pursuant to §2 of article 706-95 12 is delivered for a maximum duration of four months, renewable under the same conditions of form and length, without the total period of operations being longer than two years.

**Article 706-95-17** (created by Law n°2019-222 of 23 March 2019)**:**

The special investigative techniques established under the current Section are implemented by the judicial police officer who has been appointed by the investigating judge or who has been required by the district prosecutor, or, under his or her authority, by a judicial police agent.

In order to install, use and uninstall the technical device referred to under the current Section, the district prosecutor, the investigating judge or the judicial police officer may require any qualified agent of a service or unit or body placed under the authority or under the supervision of the Ministry of Interior or of the Ministry of Defence, a list of which is determined by means of a Decree.

**Article 706-95-18** (created by Law n°2019-222 of 23 March 2019)**:**

the district prosecutor, the investigating judge or the judicial police officer appointed by him or her or required by the public prosecutor, or the judicial police agent acting under his or her responsibility, draws-up an official record of the installation of technical devices and of

operations carried out in accordance with the current Section. This official record mentions the date and times when the operation started and the date and time when the operation ended.

The recordings are placed under closed official seals.

The judicial police officer or the judicial police agent acting under his or her responsibility describes or transcribes, in an official record filed in the criminal case file, the recorded data that are useful to ascertain the truth. No sequence relating to private life but that has no relation with penal infringements mentioned in the decisions that authorise the measure can be kept in the criminal case file.

Data in a foreign language are transcribed into French with the assistance of an interpreter appointed for this purpose.

**Article 706-95-19** (created by Law n°2019-222 of 23 March 2019)**:**

The recordings and data collected during operations carried out in accordance with the current Section are destroyed, on the request of the district prosecutor or of the public prosecutor, upon the expiry of the limitation period for prosecution. An official record is made of the destruction.

**Book IV: On some particular procedures**

**Titre XXV: Procedure applicable to organised crime and delinquency and to crimes**[147]

**Chapter II – Procedure**

**Section 6 – Other special investigation techniques**

**§2 – Collection of connection technical data and interception of correspondence sent by means of electronic communication** *(Renamed "Collection of connection data and interception of correspondence by using a technical device" in the current report)*

[147] From Article 706-73 of the Penal Procedure Code.

**Article 706-95-20** (created by Law n°2019-222 of 23 March 2019)[148]**:**

I.- A technical device or apparatus mentioned in 1° of article 226-3 of the Penal Code may be used in order to collect technical connection data that enable to identify a terminal equipment or its user's subscription number, as well as data related to the location of the terminal equipment used.

II.- This device or apparatus may be used in order to intercept correspondence sent or received by a terminal equipment. Procedures laid down in articles 100-3 to 100-7 of the current Code are applicable and, where such interception is authorised by the liberty and custody judge of the district court on the request of the district prosecutor, the powers conferred to the investigating judge or to the judicial police officer appointed by him are exercised by the district prosecutor or to the judicial police officer required by this magistrate. Correspondences intercepted pursuant to the current II can only relate to the person or to the communication link referred to in the authorisation of interception. By way of derogation from Article 706-95-16, the maximum duration of authorisations to intercept correspondence, provided for in the current II, is forty-eight hours renewable once.

The authorisation is delivered for a maximum period of fourty-eight hours, renewable once under the same conditions.

**Book IV: On some particular procedures**

**Titre XXV: Procedure applicable to organised crime and delinquency and to crimes[149]**

**Chapter II – Procedure**

**Section 6 – Other special investigation techniques**

**§4 – Remote data capture**

[148] Before law n°2019-222, a similar provision were lying in Article 706-95-4 of the Code.
[149] From Article 706-73 of the Penal Procedure Code.

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

**Article 706-102-1** (last modified by Law n°2019-222 of 23 March 2019)**:**

May be implemented a technical device aiming, without the consent of the concerned people, to access computer data, in all places, and to register, store and transmit those data, as they are stored in the computer system, or as they are displayed on the screen of the user of an automated data processing system, or as they are typed by the user of the system, or as they are received and sent by peripherals.

The district prosecutor or the investigating judge may appoint any entitled natural or legal person who is registered in one of the lists provided for in article 157, in order to perform the technical operations that allow the realisation of the technical device mentioned in the first paragraph of the current article. The district prosecutor or the investigating judge may also prescribe the use of the State's means that are covered by confidentiality for national defence purposes in accordance with the forms laid down by Chapter Ist of Title IV of Book Ist.

**Article 706-102-2** (suppressed by Law n°2019-222 of 23 March 2019)**.**

**Article 706-102-3** (last modified by Law n°2019-222 of 23 March 2019)**:**

Under penalty of nullity, the decision that authorises the use of the device referred to in Article 706-102-1 specifies the penal infringement that justifies the operation, the exact location or the comprehensive description of the automated data processing systems concerned and the duration of operations.

**Article 706-102-4** (suppressed by Law n°2019-222 of 23 March 2019)**.**

**Article 706-102-5** (last modified by Law n°2019-222 of 23 March 2019)**:**

In order to implement the technical device mentioned in article 706-102-1, the liberty and custody judge of the district court, at the request of the district prosecutor, or the investigating judge, may authorise the introduction to a vehicle or to a private place, including outside the times mentioned in article 59 of the Penal Procedure Code, without the knowledge or without the consent of the owner or of the possessor of the vehicle or of the occupier or of any person having

a right to this vehicle or place. If the device must be introduced in a home outside the times mentioned in article 59, this authorisation must be delivered by the liberty and custody judge of the district court, on the special request of the district prosecutor or by the investigating judge. These operations cannot pursue any other aim than implementing the technical device and are performed under the authority and supervision of the liberty and custody judge or of the investigating judge. The current paragraph is also applicable to operations aimed at uninstalling the technical device that has been implemented.

In order to implement the device mentioned in article 706-102-1, the liberty and custody judge of the district court, at the request of the district prosecutor or the investigating judge may also authorise the transmission of this device by means of an electronic communications network. These operations are performed under the authority and supervision of the liberty and custody judge of the district court or of the investigating judge. The current paragraph is also applicable to operations aiming at uninstalling the technical device that has been implemented.

The technical device mentioned in article 706-102-1 can neither be implemented in an automated data processing system located in places covered by articles 56-1, 56-2 , 56-3 and 56-5 , nor in the vehicle, the business premises or the home of people mentioned in article 100-7.

## PPC - Search and seizure

***Search and seizure - Flagrancy***

***Article 56 PPC – Last modified by Law n°2020-936 of 30 July 2020)***

*Where the type of the felony*[150] *is such that evidence of it may be collected by seizing papers, documents, computer data or other articles in the possession of the persons who appear to be involved in the felony or to be in possession of documents, information or articles pertaining to the criminal offence, the judicial police officer travels forthwith to the domicile of such persons to initiate a search, in respect of which he draws up an official report. The judicial police officer may also travel to any place in which are expected to be found goods whose confiscation is provided for in Article 131-21 of the Penal Code, in order to carry out there a search aiming at seizing those goods; if the search is carried out in the solely purpose of searching and seizing goods whose confiscation is provided for in § 5 and § 6 of this same Article, it must have the prior authorisation*

[150] This notion here includes misdemeanours.

*of the district prosecutor. Where the investigation is about violent offences, the judicial police officer may, either on his/her own initiative or on the instructions of the district prosecutor, seize weapons that are held by the suspected person or whose the latter has the free disposal, whatever the place these weapons lie.*

*He is the only person, together with those persons mentioned under article 57 and any persons upon whom he calls pursuant to article 60, to be allowed to examine the papers or documents or computer data before proceeding to seize them.*

*However, without prejudice to the application of Articles 56-1 à 56-5*[151]*, he has the duty first to initiate any step appropriate to ensure the observance of professional secrecy and of the defendant's rights.*

*Any article or document seized is immediately entered on an inventory and placed under official seals. However, if itis difficult to make such an inventory on the spot, they are put under temporary closed official seals until such time as an inventory can be taken and they can be placed under final official seals. This is done in the presence of the persons who have witnessed the search pursuant to the conditions set out by article 57.*

*The seizure of any computer data necessary for the discovery of the truth is carried out by placing in the hands of justice, either the physical medium holding this data or a copy of the data made in the presence of those persons present at the seizure.*

*If a copy is made, then on the orders of the district prosecutor, any computer data the possession or use of which is illegal or dangerous to the safety of persons or property may be permanently erased from any physical medium that has not been placed in judicial safekeeping.*

*With the agreement of the district prosecutor, the judicial police officer only allows the seizure of objects, documents or computer data useful for the discovery of the truth, in addition to goods which confiscation is provided for in Article 131-21 of the Penal Code.*

*Where the seizure involves money, ingots, property or securities, the preservation of which in their original form is not necessary for the discovery of the truth or for safeguarding the rights of*

[151] Articles 56-1 to 56-5 PPC organise special protection, respectively, for lawyers/barristers (a search at their home or office can only be carried out by a magistrate in the presence of the Bar President or his delegate and pursuant a written and reasoned decision taken by this magistrate, the magistrate and the Bar President are the solely persons who can consult documents before their seizure and the seizure cannot include documents or objects that relate to other infringements that are not mentioned in the above-mentioned decision – all these requirements being decreed under penalty of nullity; the Bar President or his delegate may oppose the seizure of a document or of an object, which will be settled by the liberty and custody judge), for press enterprises and journalists (a search at their home or office and cars can only be carried out by a magistrate, other rules being *mutatis mutandis* the same as those concerning lawyers), for medical doctors, notaries and bailiffs (a search at their office can only be carried out by a magistrate in the presence of the person responsible for the order or professional organisation to which the person concerned belongs, or its representative – Art. 56-3 PPC does not include any other derogations); in places identified as hosting information covered by national security (search can only be carried out by a magistrate in the presence of the President of the Commission of national security secrecy, other rules being mostly, *mutatis mutandis*, the same as those concerning lawyers), and for Courts facility and home of persons who exercise judicial functions where the search aims at seizing documents that are likely to be covered by deliberation secrecy (search can only be carried out by a magistrate in the presence of the First President of the Court of Appeal or the First President of the Court of Cassation or its delegate, other rules being mostly, *mutatis mutandis*, the same as those concerning lawyers).

*concerned persons, the district prosecutor may authorise their deposit in the Deposit and Consignment Office or at the Bank of France or on an account opened at a banking institution by the Agency for the management and recovery of seized and confiscated assets.*

*Where the seizure involves forged euro bank notes or coins (…)*

*If they are likely to provide information about objects, documents and computer data seized, the persons present when the seizure is made may be kept at the scene of the seizure by the judicial police officer for as long as is strictly necessary to complete these operations.*

***Article 57 (Last modified by Law n° 2016-731 of 3 June 2016)***

*Subject to Articles 56-1 to 56-5 and to the observance of professional secrecy and of the defendant's rights referred to in Article 56, the operations prescribed in that article are made in the presence of the person in whose domicile the search is made.*

*Where this is impossible, the judicial police officer has the duty to ask him to appoint a representative of his choice; failing this, the judicial police officer will appoint two witnesses, chosen for this purpose from among persons who are not under his administrative authority.*

*The official report of these operations is drafted as described under article 66 and is signed by the persons mentioned by the present article; in the event of a refusal, this is noted in the official report.*

***Article 57-1 (Last modified by Law n°2016-731 of 3 June 2016)***

*Judicial police officers or judicial police agents under their supervision may, during the course of a seizure carried out in the conditions laid down by the present Code, access, through a computer system set up within the premises where the seizure is carried out, any data relevant to the inquiry in progress and stored in the said system or in another computer system, provided that this data is accessible from the initial system or available for the initial system.*

*They may also, under the conditions provided for in the current Code, access through a computer system set up in the premises of a Police or Gendarmerie service or unit, to data relevant to the inquiry in progress and stored in another computer system, provided that this data is accessible from the initial system.*

*Where it is known in advance that data which is accessible from the initial system or available for the initial system, is stored in another computer system situated outside the territory of the French Republic, it is collected by the judicial police officer, subject to the conditions of access provided by any international agreements in force.*

*The data which has been accessed pursuant to the conditions of the present article may be copied onto any medium. Any computer storage equipment may be seized and placed in judicial safekeeping under the conditions laid down by the present Code.*

*Judicial police officers may, by any means, require any person who is likely:*

*1° To have knowledge of measures applied in order to protect the data to which it is authorised to access within the framework of the search;*

*2° To provide them with information that enable to access data mentioned in §1°.*

*With the exception of persons referred to in articles 56-1 to 56-5, refraining from responding as soon as possible to this requisition is punished by a fine of 3 750 €.*

***Article 58 (Last modified by Ordonnance n°2000-916 of 19 September 2000)***

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

*Subject to the necessities of inquiries, any communication or disclosure of a document seized during a search to a person not lawfully accredited to examine it, made without the authorisation of the person under judicial investigation or his successors, or that of the signatory or addressee of the document, is punished by a fine of €4,500 and imprisonment for up to two years*

***Article 59 (Last modified by Law n° 93-1013 of 24 August 1993)***

*Except where they are requested from within a building or in the exceptional cases provided for by law, searches and house visits may not be undertaken before 6 a.m. or after 9 p.m.*

*The formalities mentioned under articles 56, 56-1, 57 and the present article are prescribed under penalty of nullity.*

***Article 60 (Last modified by Law n°2019-222 of 23 March 2019)***

*Where there is occasion to carry out any technical or scientific examination, the judicial police officer, or under the supervision of the latter, the judicial police agent, has recourse to all qualified persons.*

*Unless they are registered on one of the lists provided for by article 157, the persons called upon take an oath in writing to assist the administration of justice upon their honour and conscience.*

*The persons appointed to carry out any technical or scientific examination may open the official seals. They draw up an inventory and mention this in a report made in compliance with the provisions of articles 163 and 166. These persons may also, provided they mention it in their report, replace under seal the objects that were examined and place under seal the objects that result from their examination; In particular, medical doctors required in order to make an autopsy or a medical examination may place under seal the samples taken from examination. They may orally communicate their findings to the investigators in cases of emergency.*

*On the instructions of the district prosecutor, the judicial police officer or, under the supervision of the latter, the judicial police agent, discloses the findings of the technical and scientific examinations to those persons against whom matters exist giving rise to the suspicion that they have committed or have attempted to commit offences, and also to the victims.*

***Article 60-1 (Last modified by Law n°2019-222 of 23 March 2019)***

*The district prosecutor or the judicial police officer or, under the latter's supervision, the judicial police agent, may by any means order any person, establishment or organisation, whether public or private, or any public services likely to possess any documents relevant to the inquiry in progress, including those produced from a computer system or a personal data processing system, to provide them with this information, in particular in digital form, where needed in compliance with norms established by regulation, Without legitimate grounds, the duty of professional secrecy may not be given as a reason for non-compliance. Where such orders relate to the persons mentioned in articles 56-1 to 56-5, the transfer of the information may only take place with their consent.*

*With the exception of the persons mentioned in articles 56-1 to 56-5, the failure to respond to such an order as quickly as possible is punished by a fine of €3,570.*

*Under pain of nullity, cannot be included in the case file an information gathered based on an order taken in violation of Article 2 of Law of 29 July 1881 on press freedom.*

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

***Article 60-2 (Last modified by Law n°2019-222 of 23 March 2019)***

*At the request of the judicial police officer, or, under the supervision of the latter, of the judicial police agent, intervening by means of telecommunications or computers, public organisations or private legal persons, with the exception of those set out in paragraph 2 d of Article 9 of the EU Regulation 2016/679 of 27 April 2016 and in paragraph 2 of Article 80 of Law no. 78-17 of 6 January 1978 relating to computers, files and liberties, must make available information helpful for the discovery of the truth, with the exception of information the secrecy of which is protected by law, where it is stored in one or more computer or personal data processing systems that they administer.*

*The judicial police officer, or, under the supervision of the latter, of the judicial police agent, intervening on the orders of the district prosecutor authorised in advance by a decree from the liberty and custody judge, may require telecommunications operators, particularly those mentioned in 1 of I of article 6 of Law no. 2004-575 of 21 June 2004 relating to confidence in the digital economy, to take without delay all appropriate measures to ensure the preservation, for a period that may not exceed one year, of the text of the information consulted by persons using the services provided by the operators.*

*The organisations or persons to which this article applies must make the required information available as quickly as possible by telematic or electronic means.*

*Refusal to respond to such a request without a legitimate reason is punished by a fine of €3,750.*

*A Decree of the Conseil d'Etat made on the advice of the National Commission for Data Protection determines the categories of organisation covered by the first paragraph, and also the methods for examining, transmitting and processing the required information.*

***Article 60-3 (Last modified by Law n° 93-1013 of 24 August 1993)***

*Where have been sealed objects that are computer data storage medium, the district prosecutor or the judicial police officer or, under the latter supervision, the judicial police agent, may, by any means, require any qualified person registered on one of the lists provided for in Article 157 or having swear in writing the oath provided for in Article 60, to carry out the opening of judicial seals in order to make one or several copies of the data so that they can be used without undermining their integrity. The required person mentions operations that have been carried out in a report established in compliance with Articles 163 and 166.*

***Search and seizure - Preliminary investigation***

***Article 75-2 PPC (Last modified by Law n° 2000-516 of 15 June 2000)***

*The judicial police officer carrying out a preliminary inquiry into a felony or misdemeanour informs the district prosecutor as soon as a person has been identified against whom there is evidence that he has committed or attempted to commit an offence*

***Article 76 PPC (Last modified by Ordonnance n° 2019-964 of 18 September 2019)***

*Searches, house visits and seizures of exhibits or of goods whose confiscation is provided for in Article 131-21 of the Penal Code may not be made without the express consent of the person in whose residence the operation takes place.*

*Such consent must be made in the form of a hand-written statement by the person concerned or, if the person cannot write, this is noted in the official report, together with his consent.*

*The provisions set out in articles 56 and 59 of the current Code are applicable.*

*If the needs of an inquiry into a felony or a misdemeanour punished by a prison sentence of three years or more or the search for goods whose confiscation is provided for in Article 131-21 of the Penal Code justify this, the liberty and custody judge of the first instance court may, at the request of the district prosecutor, decide, in a written and reasoned decision, that the operations provided for by the present article will be carried out without the consent of the person in whose residence they take place. On pain of nullity, the custody judge's ruling states the qualification of the offence for which the evidence is being sought, as well as the address of the places in which these operations may be carried out. This decision is reasoned with reference to the legal and factual matters which justify the necessity for these measures. The operations are carried out under the supervision of the judge who ordered them, who may travel to the places in question to ensure that the legal provisions are observed. On pain of nullity, these measures may serve no purpose other than the seeking out and detection of the offences outlined in the custody judge's ruling or the seizure of goods whose confiscation id provided for in Article 131-21 of the Penal Code. However, if these operations reveal offences other than those outlined in this ruling, this does not constitute grounds for nullity in relation to proceedings in respect of them.*

*For the application of the provisions of the preceding paragraph, the liberty and custody judge of the district court whose prosecutor leads the investigation is competent, whatever the territorial jurisdiction in which the search will take place. The liberty and custody judge may then travel to the location wherever on the national territory it may be. The district prosecutor may also refer the matter to the liberty and custody judge of the district court in the territorial jurisdiction where the search will take place, through the intermediary of the district prosecutor of that court.*

***Article 76-3 PPC (Last modified by Law n° 2003-239 of 18 March 2003)***

*The police officer may, for the needs of the inquiry, have recourse to the processes provided for by article 57-1, pursuant to the terms of article 76.*

***Article 77-1 PPC (Last modified by Law n° 2019-222 of 23 March 2019)***

*If any technical or scientific reports or examinations need to be carried out, the district prosecutor, upon the latter's authorisation, a judicial police officer or agent, may call upon any qualified person.*

*The provisions of the second, third and fourth paragraphs of article 60 are applicable.*

***Article 77-1-1 PPC (Last modified by Law n° 2019-222 of 23 March 2019)***

*The district prosecutor or, upon the latter's authorisation, the judicial police officer or agent, may, by any means, order any person, establishment or organisation, whether public or private, or any public services who or which is likely to possess any information relevant to the investigation, including those produced from a computer or personal data processing system, to provide them with these documents, including in digital form, where needed in compliance with regulatory standards. Without legitimate grounds, the duty of professional secrecy may not be given as a*

*reason for non-compliance with such an order. Where these orders relate to the persons mentioned in articles 56-1 to 56-5, the transfer of these documents may only take place with their consent.*

*Where the person does not respond to this order, the provisions of the second paragraph of article 60-1 are applicable.*

*The last paragraph of Article 60-1 is also applicable.*

***Article 77-1-2 PPC (Last modified by Law n° 2019-222 of 23 March 2019)***

*Upon the district prosecutor's authorisation, the judicial police officer or agent may issue the demands provided for by the first paragraph of article 60-2.*

*Upon the authorisation of the liberty and custody judge, seized for this purpose by the district prosecutor, the judicial police officer or agent may issue the demands provided for by the second paragraph of article 60-2.*

*The organisations or persons concerned must put the required information at their disposal by telematic or electronic means as quickly as possible.*

*Refusal to respond to these demands without legitimate grounds is punished in accordance with the provisions of the fourth paragraph of article 60-2.*

***Article 77-1-3 PPC (Created and last modified by Law n° 2019-222 of 23 March 2019)***

*Upon the district prosecutor's authorisation, the judicial police officer or agent may issue the demands provided for in Article 60-3.*

***Search and seizure – Judicial information***

***Article 92 PPC (Last modified by Law n° 91-646 of 13 July 1991)***

*The investigating judge may go to the scene of the offence to make any useful findings or conduct a search. He informs the district prosecutor who is entitled to accompany him.*

*The investigating judge is always accompanied by a clerk.*

*He drafts an official record of all his operations.*

***Article 94 PPC (Last modified by Law n° 2010-768 of 9 July 2010)***

*Searches are made in all the places where may be found objects or computer data which could be useful for the discovery of the truth.*

***Article 95 PPC (Last modified by Law n° 93-2 of 4 January 1993)***

*If the search is made in the domicile of the person under judicial examination, the investigating judge must comply with the provisions of articles 57 and 59.*

***Article 96 PPC (Last modified by Law n° 2016-731 of 3 June 2016)***

*If the search is made in a domicile other than that of the person under judicial examination, the person in whose domicile it must be made is invited to attend. If this person is absent or refuses to attend, the search is made in the presence of two of his relatives or relatives by marriage present on the premises or, failing which, in the presence of two witnesses.*

*The investigating judge must comply with the provisions of articles 57 (second paragraph) and 59.*

*However, he has the duty to organise in advance all the appropriate measures to ensure the observance of professional secrecy and the defendant's rights.*

*The provisions of articles 56 and 56-1 to 56-5 apply to searches carried out by the investigating judge.*

***Article 97 PPC (Last modified by Law n° 2019-222 of 23 March 2019)***

*Where in the course of an investigation there is a need to search for documents or electronic data, and subject to the requirements of the investigation and compliance, where necessary, with the obligation imposed by the third paragraph of the previous article, the investigating judge or the judicial police officer commissioned by him has the sole right to examine such documents before carrying out the seizure.*

*An inventory is made of all objects, documents and computer data placed in judicial safekeeping, which are immediately placed under official seals. However, if this is difficult to do on the spot, the judicial police officer proceeds as indicated under the fourth paragraph of article 56.*

*The seizure of any computer data necessary for the discovery of the truth is carried out either by seizure of the physical medium in which the data is held or by means of a copy of the data made in the presence of those persons who were present at the seizure.*

*If a copy is made within the framework of this procedure, then on the orders of the investigating judge, any computer data the possession or use of which is illegal or dangerous to the safety of persons or property may be permanently erased from any physical medium that has not been placed in judicial safekeeping.*

*With the agreement of the investigating judge, the judicial police officer only maintains the seizure of objects, documents or computer data useful for the discovery of the truth, in addition to goods whose confiscation is provided for in Article 131-21 of the penal Code.*

*If these official seals are closed, they may be opened and the documents examined only in the presence of the person under judicial examination in the presence of his advocate, or where the both have been duly summoned. However, where the opening and the reconstruction of the closed seal do not require that the accused person be questioned in relation to its content, they may be carried out by the investigating judge assisted by his clerk without the presence of this accused person, with the presence of its lawyer or the latter duly summoned.*

*Unless the needs of the investigation prevent it, a copy or photocopy of the documents or computer data placed under judicial safekeeping may be delivered as soon as possible to any persons concerned who request it at their own expense.*

*If the seizure comprises monies, ingots, papers or securities which do not necessarily have to be preserved in kind for the discovery of the truth or for the safeguarding of the rights of the parties, he may authorise the clerk to deposit them in the Deposit and Consignment Office or at the Bank of*

*France or on an account opened at a banking institution by the Agency for the management and recovery of seized and confiscated assets.*

*If the seizure comprises counterfeit banknotes or coins, the investigating judge or the judicial police officer committed by him must provide, for analysis and identification, with at least one example of each type of coin or banknote suspected of being fake, to the national analysis centre empowered for this purpose. The national analysis centre may proceed to open any seals. It makes a list in a report which must record any opening or reopening of the seals. When operations are complete, the report and the seals must be put into the hands of the clerk in the relevant court of law. An official record is made of their being so deposited.*

*The requirements of the preceding paragraph do not apply in cases where there is only one suspected fake coin or note, and this is needed to establish the truth.*

***Article 97-1 PPC (Last modified by Law n° 2019-222 of 23 March 2019)***

*Where this is necessary to comply with a rogatory letter, the judicial police officer may carry out the measures provided for in article 57-1.*

***Article 98 PPC (Last modified by Law n° 2000-916 of 19 September 2019)***

*Subject to the requirements of the judicial investigation, any communication or disclosure made without the authorisation of the person under judicial examination or that of his beneficiaries or of the signatory or addressee of a document found during a search, to a person not authorised by law to examine it, is punished by a €4,500 fine and two years' imprisonment.*

***Article 99 PPC (Last modified by Law n° 2019-222 of 23 March 2019)***

*During the investigation, the investigating judge is competent to decide on the restitution of articles placed under judicial authority.*

*He decides by a making a reasoned order either upon the district prosecutor's submissions or, after hearing the prosecutor's opinion, on his own motion or upon the application of the person under judicial examination, the civil party or any other person claiming a right over the article. Where the request is made in compliance with the penultimate paragraph of Article 81, because the investigating judge did not take his decision within a period of one month, the person may directly bring the matter before the president of the investigation chamber, for judgment in accordance with the three last paragraphs of Article 186-1.*

*He may also on its own motion decide, with the agreement of the district prosecutor, to return or to have returned to the victim of the offence the articles placed under judicial authority whose ownership is not disputed.*

*No restitution is made where it is liable to hinder the discovery of the truth or the safeguard of the rights of the parties, or where the seized item is the instrument or the direct or indirect product of the infringement or where it creates a danger for persons or for property. It may be refused when the confiscation of the article is provided for by law.*

*The investigating judge's order under the second paragraph of the current article is notified either to the applicant in the event of a dismissal of the application, or to the public prosecutor and to any*

*other party concerned in the event of a restitution decision. It may be referred to the president of the investigating chamber or to the investigating chamber by an ordinary application submitted to the clerk of the court within the time limit and according to the conditions set out by the fourth paragraph of article 186. This time limit is suspensive.*

*The third party's observations may be heard by the president of the investigating chamber or by the investigating chamber, as well as those of the parties, but this third party may not ask for the case file to be put at his disposal.*

***Article 99-3 PPC (Last modified by Law n° 2016-731 of 3 June 2016)***

*The investigating judge or the judicial police officer committed by him may order any person, establishment or organisation, whether public or private, or any public services liable to possess any documents relevant to the investigation, including those produced from a computer or personal data processing system, to provide them with these documents, including in digital form. Without legitimate grounds, the duty of professional secrecy may not be given as a reason for non-compliance with such an order. Where these orders relate to the persons mentioned in articles 56-1 to 56-3 and in Article 56-5, the transfer of these documents may only take place with their consent.*

*Where the person does not respond to this order, the provisions of the second paragraph of article 60-1 are applicable.*

*The last paragraph of Article 60-1 is also applicable.*

***Article 99-4 PPC (Last modified by Law n° 2004-204 of 9 March 2004)***

*Where necessary to carry out a rogatory commission, the judicial police officer may issue the demands provided for by the first paragraph of article 60-2.*

*With the express permission of the investigating judge, the judicial police officer may issue the demands provided for by the second paragraph of article 60-2.*

*The organisations or persons concerned must put the required information at their disposal by telematic or electronic means as quickly as possible.*

*Refusal to respond to these demands without legitimate grounds is punished in accordance with the provisions of the fourth paragraph of article 60-2.*

***Article 99-5 PPC (Created and last modified by Law n° 2016-731 of 3 June 2016)***

*For the needs of the execution of the letter of Request, the judicial police officer may, with the express authorization of the investigating judge, issue the demands provided for in Article 60-3.*