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

Introductory questions:

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

Answer: Indication of length of answer: one line.

ECIJA LAW FIRM. Compliance and Criminal Law Partner

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

Answer: Indication of length of answer: one line.

Located in Spain, with headquarters in Madrid. Also, offices in Portugal, USA, Chile, Panamá, Costa Rica, Honduras, Dominican Republic, Guatemala, El Salvador, Mexico, Ecuador, Brazil and Puerto Rico,

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: Indication of length of answer: couple of lines

In accordance with Circular 5/2019 of 6 March from the Public Prosecution Service on the registration of computer devices and equipment, the mass information storage devices referred to in articles 588 *sexies* a to 588 *sexies* c of the Criminal Procedure Act (LECrim) shall include not only instruments capable of recording, storing and subsequently recovering or reading digital information, but also the media used to do so.

It is also necessary to mention what the legal regulation calls telematic communication instruments, which would be all those devices that, in some way, intervene in remote communications that may take place through computer means. Although this would include computers and mobile phones specifically included in the legal provision, the regulation would also cover other devices, such as routers, which, while facilitating telematic communications, can provide interesting data to a criminal investigation.

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

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

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

Mobile device not seized

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

As a consequence of the approval in Spain, on October 5, 2015, of the Organic Law 13/2015 on the modification of the Law of Criminal Procedure for the strengthening of the procedural guarantees and the regulation of the technological research measures, the regulation of the registry of the devices and computer systems is included in our legislation.

Both Law 13/2015 and the subsequent Circular 5/2019 of the Attorney General's Office emphasize the importance and the need of protecting the fundamental rights of individuals which may be affected by this issue. These rights are essentially the ones recognised by the Spanish Constitution in article 18 regarding the Right to honour, privacy and own image.

However, the legislator has contemplated certain cases, where the access is allowed without the judicial authorization:

1. **Consent of the Owner**: The consent of the person under investigation to the seizure of electronic devices may be express or tacit, the latter being understood as consent that does not result from expressions but from facts (conclusive acts).

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

Article 551 LECrim refers to the consent for the practice of the diligence of entry and registration indicating that it will be understood that consent is given , if once the request is made, the individual in question executes on his part the necessary acts that depend on him so that they can have effect, without invoking the inviolability the State recognizes to the domicile" (article 18.2 Spanish Constitution).

The jurisprudence of the Constitutional Court, in rulings such as STC 173/2011, November 7, 2011, states that the effective consent of the subject allows for the intrusion of his or her right to privacy, since each person determines the scope of personal and family privacy that he or she reserves to the knowledge of others. This consent may be revoked at any time, and furthermore the permitted intrusion may not extend the scope for which it was granted, since it would break the relationship between the personal information that is collected and the tolerated purpose for which it was collected.

However, the simple lack of opposition to the registry (in this sense, STC No. 209/2007, of 31 September, regarding a home search) cannot be admitted as tacit consent, and at least acts that manifest an unequivocal will to collaborate with the registry are required, as would be, for example, the case described in STS No. 786/2015, of 4 December, in which it was admitted this tacit will, based in the act of providing the police with the identity of the e-mail accounts and passwords. STS no. 864/2015, of December 10, in turn, considered valid the tacit consent to the analysis of a computer derived from the authorization to the police to collect it, considering "it is unquestionable that the authorization to collect involves the analysis of the content found in said computer material". Also, the procedure of STC No. 173/2011, of 7 November, in which consent is understood to have been given by handing over a computer that lacks a password.

Likewise, consent must be free and unvitiated since, as stated in STS No. 1576/1998, of 11 December, "it must be free of any element that might provoke or constitute error, violence,

intimidation or deceit (art. 1.265 of the Civil Code), since if such strict requirements are required for contractual relations, much more severity must be applied when it comes to renouncing a fundamental right of the individual". In this context, it should not be forgotten that the last paragraph of article 588 sexies c specifically prohibits the authorities and agents responsible for the inquiry from compelling the person under investigation or prosecuted to collaborate in the registration of the device.

In those cases in which the affected person is arrest, applying the jurisprudential doctrine developed for cases of house searches, the assistance of legal counsel will not be required to carry out the search of the device, but it will be necessary to obtain the consent of the affected person, if there is no judicial authorization (STS no. 187/2014, of 10 March). "*The reason for this," states STS 550/2001, of 3 April, "is that the expression of will thus provide must be seriously questioned, taking into account that the detainee may feel conditioned or pressured by such a situation, even unaware of the possibility of refusing to authorize entry, as well as the consequences that may derive from such an act".*

2. **Urgent Cases**: Article 588 sexies c.4 has introduced in the Criminal Procedure Act an issue that had already been contemplated for a significant time by the jurisprudential doctrine. This, is the possibility that the Judiciary Police may register mass information storage devices **without prior judicial authorization** in urgent cases where, in addition, a legitimate constitutional interest makes the measure essential and, always, with subsequent validation by the judge.

   The mentioned article states:

   "In urgent cases where a legitimate constitutional interest is appreciated which makes the measure provided for in the previous paragraphs of this article essential, the Judiciary Police may carry out a direct examination of the data contained on the confiscated device, notifying the competent judge immediately and, at any event, within a maximum of twenty-four hours, in a reasoned writ, recording the reasons justifying adoption of the measure, the proceedings carried out, the manner

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

in which it was effected and its result. The competent judge, also in a reasoned manner, will revoke or confirm such action within a maximum time limit of 72 hours after the measure was ordered.

Therefore, and after the reform of the Criminal Procedure Act in 2015, police access without prior judicial authorization is legitimized to data that affect not only the right to privacy (18.1 CE), but also the fundamental right to secrecy of communications (18.3 CE), when the requirements of urgency and necessity established in the above article are met. The previous judicial restrictions on the fundamental right established in article 18.3 CE does not require a prior judicial decision anymore (as long as we are under the above mention exception), but simply a judicial decision which, for that reason, may be subsequent or valid. Thus, the legislator, aware that the registration of a mass storage device, such as a smartphone or a personal computer, will normally contain data affecting the secrecy of communications, has allowed it to be registered by the police in exceptional cases, subject to the necessary judicial validation.

So, after the reform, the fundamental rights than can be affected by the registration of a storage or mobile device have gone from being consider individually, to contemplating what has been called the right to a person's virtual environment, which is a new reality that demands unitary processing (see STS No. 204/2016, of 10 March).

The validity of the registration, prior to having a judicial authorization, is conditioned to the concurrence of four requirements: urgency, legitimate constitutional interest that makes the measure essential, subsequent communication to the judge in the form and terms that are established and subsequent judicial validation of the measure.

(i) The **urgency** that justifies police interference in people's privacy without prior judicial authorization is addressed in the STC No. 70/2002 of 3 April, as necessary for the prevention and investigation of a crime, the discovery of criminals and the collection of incriminating evidence. For example, STC no. 115/2013, of 9 May, understood that the intervention was urgent due to the need to find out the identity of some of the people

who ran when they were caught red-handed, guarding an important drug stash, thus avoiding that they could escape the action of Justice.

(ii) The **legitimate constitutional interest** must be based on the fact that the admissibility of the interference of the public authority into the right to privacy requires that the purpose of the measure is one of the followings: national security, public safety, the economic well-being of the country, the defence of order and the prevention of crime, the protection of health or morals, or the protection of the rights and freedoms of others. Among them, the fight against crime is usually the one which legitimate the police action.

(iii) **The communication to the judge** that the Judiciary Police must meet two requirements, one temporal and one formal.

a. The temporal requirement determines that the communication has to be made within a maximum period of 24 hours. It will be necessary, therefore, to provide a record of the search, including the exact date and time at which the police search was carried out. The legal timeframe will be counted from the time the search takes place until the time of presentation to the court, which will be formally established by a diligence of record or minute that will be raised to that effect.

b. As formal requirements, the Law demands that the police communication is made to the competent Judge by means of a written document that includes the reasons that justified the adoption of the measure, the concrete action carried out, the method in which it has been carried out and its result. Within these reasons, the Judiciary Police will have to include the motives of urgency that led to the action in question, which will later be included in the judicial ruling of validation, as long as the judge considers them sufficient to validate the measure.

This provision does not prevent the judge from requiring the police to issue a new report in addition to the previous one when the one submitted does not meet the requirements.

(iv) **The court ruling that validates or revokes the measure** must be issued by the Judge within a maximum of 72 hours, counting not from the time of its notification to the

court, but from the time when the action was carried out, hence the importance of recording the day and time when the search is carried out, as indicated above. The court ruling validating the measure must have the same basis as it would have had without the prior police search, but it must add the assessment and consideration of the relevance of the prior police intervention. Therefore, the judge will have to **justify the** concurrence of the guiding principles and, among them, especially the proportionality and necessity of the measure in the specific scenario in which it has been adopted, that is, prior to judicial intervention, in view of the urgency of the case.

It will also be necessary to comply with the above mention requirements, when the devices have been searched independently of a house search. For example, where on the occasion of an arrest - or without the need for one - the police occupy the mobile phone of a suspect or the geolocation device of a vehicle involved in a serious accident or, ultimately, the computer of the person under investigation in a criminal act.

The ex post finding of the absence of enabling requirements, or the failure to respect the principle of proportionality, would imply the violation of a fundamental right and would have procedural effects in terms of the illegal nature of the evidence, obtained by violating fundamental rights. Thus, being inadmissible in court.

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

The basic principle under which these devices can be seized, read, accessed, and/or analysed is based on a judicial authorization and only under the above mention circumstances, they can be trespassed upon. This, because the legal system is protecting fundamental rights recognised in the Spanish Constitution.

So, as stated in the previous answer the limits are the rights recognised in article 18 of the constitution regarding the Right to honour, privacy and own image.

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

(i) Art. 18.1: *The right to honour, personal and family privacy and own image is guaranteed.*

(ii) Art 18.3: *"The secrecy of communications and, in particular, of postal, telegraphic and telephone communications, is guaranteed, except in the event of a court order.*

(iii) Art. 18.4: *"The law shall limit the use of computer science in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights.*

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

Again, we must refer to the answer given to question 4, since it is not specified in the law that the device cannot be accessed by technological tools, or any particular tool when the search is done without a prior court order.

However, it should be noted that the law does provide that the judicial authorization may delimit the scope of the search in relation to the specific technical tool to be used. As such, the fact that an investigation is authorized to search all the data stored in a particular device does not mean that the privacy of all such data will be accessed. Indeed, there are forensic tools that use search engines to find certain files on a computer or computer system without having to display the content of all the files searched. That way, the privacy of the affected individual is safeguarded.

Consequently, provided that the principle of proportionality and the requirements justifying the measure and tools used are met, these may be validated ex post by the competent judge.

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

There is no legal provision against making copies. Again, any action taken under the circumstances described in the answer to question 4 must be duly justified under the principle of proportionality and always in compliance with the requirements described.

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

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

As stated, the consent will be required unless we have a judicial authorisation signed by the competent judge or else, we act under the assumption of urgency described above.

If the owner is a company and the person in possession an employee of the company, policies about the use of organization equipment must be taken into account.

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

There is, and it is stated in the Constitution the duty to collaborate with judges (art. 118). Accordingly, article 588.sexies.c and article 19 of the Budapest Convention call on the States Parties to adopt such legislative and other measures as may be necessary to empower their competent authorities to order any person who has knowledge of how computers system works to supply all necessary information.

The duty of cooperation imposed is, however, subject to certain limits in the LECrim. It is possible to speak of a subject limitation, which would restrict individuals from whom collaboration may be demanded, and an objective limitation, which exempts from the duty when collaboration is particularly burdensome.

As for the subject limitation, **the provision expressly excludes from the duty to collaborate the person investigated or prosecuted,** his closest relatives and those who, in accordance with the provisions of art. 416.2 LECrim, are exempted from the obligation to declare by virtue of professional secrecy. The dispensation granted to the investigated or accused person is a logical consequence of the scope of his own right of defence and the power derived from it, which allows him not to testify against himself.

So, no individual can be force to unblock the device without the proper judicial authorisation, and, taking into account we cannot get consent without the presence of an attorney and we

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

cannot invoke the duty to collaborate, since the prosecuted has his own right of defence, we understand if the owner is under investigation or prosecuted it cannot be forced to unlock the device.

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

Not necessary if the proper judicial authorisation has been given

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

The Judiciary Police.

As we speak about mobile devices which aren`t already seize, there are not formal requirements related to the request of authorisation since we would be facing a case of urgency or consent of the owner.

However, it is important to highlight that regarding urgent cases, all the requirements and formalities set out in the answer to question 4 must be fulfilled:

- Proportionality of the measure and justified urgency
- Legitimate Constitutional interest
- Communication to the competent judge 24 hours after the search, meeting the formal requirements of the communication (see answer to question 4)
- The subsequent validation of the measure, from the competent judge

Also, regarding the consent of the owner it is imperative to respect the already exposed limits, and no consent of the owner will be admissible if the person is arrested and its attorney is not present.

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

Every individual enjoys the protection granted by the fundamental rights contained in the Constitution.

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

However, we need to take into consideration two nuances:

1. Regarding the obligation of collaboration there is a subject limitation, where the LECrim **expressly excludes from the duty to collaborate the person investigated or prosecuted,** his closest relatives and those who, in accordance with the provisions of art. 416.2 LECrim, are exempted from the obligation to declare by virtue of professional secrecy.

2. If the individual is being accused, investigated or prosecuted, among the protected rights of honour, privacy and own image, it also has the right to its own defence. This impacts directly in the consent of the owner, which will be inadmissible, if it has been granted without the presence of a lawyer.

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.*

Access to external computer systems may raise issues of jurisdiction. Indeed, the absence of borders on the Internet, coupled with the lower costs of service in certain countries, will often mean that data storage servers are physically located outside the territory in which the judge authorising the registration exercises jurisdiction (or even the place where they are located is unknown). In these cases, if one starts from a traditional conception of the limits of jurisdiction based on territorial criteria, it might seem more correct to resort to international judicial cooperation mechanisms to obtain such data, which, however, would be absolutely incompatible with the speed required for this type of investigation.

Furthermore, in many cases, either the location of the data is unknown (offshoring) or the data are fragmented in servers located in various territories or their location in one or another place

is beyond the control of the data subject and depends exclusively on the technical or operational convenience of the storage service provider that changes the location according to its own needs. Therefore, making the collection of data conditional on the location of the data would lead to the failure of many investigations simply because the exact location of the data is unknown, thus rendering the international cooperation measures adopted ineffective.

In view of this perspective, the Spanish legislator has decisively opted for the legality of access with simple judicial authorisation, even in cases where the data are located outside Spain. This is evident from the literal interpretation of the legal regulation, and even more so, if it is compared with the immediate precedent, article 350.4 of the Proposed Criminal Procedure Act, which limited access to data stored in computer systems located in Spanish territory, referring to international judicial cooperation in the rest of the cases. This provision followed the criteria of art. 19.2 of the Convention on Cybercrime that, in its Explanatory Report, expressly stated that the rule did not allow the registration of systems located outside the national borders, referring also to international judicial cooperation for these cases.

The approach now being taken, however, is to consider telematic storage repositories as a further part of the system being recorded. What matters is not where the data are physically located, but where they are accessed from.

So, it can be stated that if the owner access these data from Spain and exercises his rights over them from Spain and in accordance with Spanish law, it can be stated that when the access it is done from Spain and in accordance with Spanish law provided, of course, that, as has been pointed out, one can speak of legal access.

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

If we speak to the proportionality of the measure, in accordance with the general criteria established in the LECrim, to assess the case in question, the judge will have to state the legal framework that justified the sacrifice of the rights and interests of the person concerned. Thus,

for example, in cases of particularly serious offences, where the life of a person or public security is at stake (as would be the case with terrorist offences), the particular interests of the individual must normally be ceded. On the other hand, in the case of minor offences or where the data which the search may provide to the investigation are not particularly decisive, the interests of the individuals must be assessed more strongly. For the above purposes, in Spain, those offences that are punishable by a prison term of more than 5 years are considered grave offences.

For the same reason, we can also mention the Law, 25/2007, of 18 October, on the conservation of data relating to electronic communications and public communications networks, which aims to regulate the obligation of operators to retain data generated or processed in the context of the provision of electronic communications services or public communications networks, as well as the duty to transfer such data to authorised agents whenever they are required to do so by means of the corresponding judicial authorisation for the purpose of detecting, investigating and prosecuting grave offences under the Criminal Code or special criminal laws. So, it can be understood, that if we are before minor offences the rights to privacy and own image may be protected.

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.*

Yes, that situation will always lead to the inadmissibility in court of the evidence.

Mobile device seized

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

Where, due to the search of a domicile being made, it is foreseeable that computers, telephone or online communication instruments or mass digital information storage devices or access to online data warehouses will be seized, the Examining Magistrate's decision must extend its

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

grounds to justification, as appropriate, of the reasons legitimising access by the agents empowered to the information contained on such devices.

Simple confiscation of any of the devices referred to in the previous paragraph, carried out while the search warrant for the domicile is in progress, does not legitimise access to their content, without prejudice to the fact that such access may be authorised subsequently by the competent judge.

Regarding the access to the information on electronic devices confiscated outside the domicile of the party under investigation, the requirement provided for in paragraph 1 will also be applicable to cases where computers, communications instruments or mass data storage devices, or access to online data warehouses, are seized independently of a house search. In these cases, the agents will make the confiscation of such effects known to the judge. If the judge considers access to the information housed in their content is essential, they will grant the relevant authorisation.

To this respect, it is important to highlight that when we talk of the seize of devices out of house search, for example where on the occasion of an arrest - or without the need for one - the police occupy the mobile phone of a suspect or the geolocation device of a vehicle involved in a serious accident or, ultimately, the computer of the person under investigation in a criminal act, the judicial authorization, is only for the search or analysis of the content of the device, but not for its seizure or confiscation, which does not require prior judicial authorization. Thus, in the case of the judicial police, the collection of the effects, instruments or evidence of the offence will constitute one of its tasks and, at the same time, obligations; art. 282 LECrim:

> *"The Judiciary Police's purpose, and obligatory on all those who are a part of it, is to verify public crimes committed in its territory or division; take, depending on their powers, the necessary legal measure to ascertain them and discover who the offenders are, and collect, for all purposes, instruments or evidence of the crime which may be in danger of disappearing, placing them at the disposal of the judicial authority. Where the victims come into contact with the Judiciary Police, it will comply with the duties of disclosure provided for by current legislation. Furthermore, they will*

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

assess the personal circumstances of the victims to decide what protection measures should provisionally be adopted to ensure their proper protection, without prejudice to the final decision which must be taken by the Judge or Court."

- Limits:

The LECrim, art. 588 sexies c 2 establishes, that except where they constitute the object or instrument of the crime, or there are other reasons to justify it, confiscation of hardware containing computer data or files will be avoided where this may cause serious prejudice to their holder or owner and it is possible to obtain a copy of them under conditions which guarantee the authenticity and integrity of the data.

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

During instruction of the procedures any of the investigative measures regarding Communal provisions for interception of telephone and telematic communications, capture and recording verbal communications with the use of electronic devices, use of technical devices for image surveillance, location and capture, search of mass data storage devices and remote searches of computer equipment may be ordered, as long as judicial authorisation is issued fully subject to the principles of speciality, adequacy, exceptional nature, necessity and proportionality of the measure.

The mention measures must be order by the competent judge ex officio, or at the request of the Public Prosecution Service or the Judiciary Police.

Where the Public Prosecution Service, or the Judiciary Police, apply to the Examining Magistrate for a technological investigation measure, the application must contain:

1. The description of the event under investigation and the identity of the person under investigation, or any other affected by the measure, as long as this data is known.

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

2. A detailed description of the grounds justifying the need for the measure in accordance with the guiding principles provided for in article 588 a. i., and the evidence of criminality which was discovered during the investigation prior to the application to authorise the interception.

The application for authorisation must algo contain:

- The identification data of the accused and, as appropriate, the means of communication used which allow enforcement of the measure.
- The extent of the measure and specification of its content.
- The investigation unit of the Judiciary Police that will be in charge of the intervention.
- The manner in which the measure will be enforced.
- The duration of the measure applied for.
- The person in charge of carrying out the measure, if known.

In relation with the judicial decision, the examining magistrate will authorise or refuse the measure applied for with a reasoned order, having heard the Public Prosecution Service. This decision will be issued within a maximum of twenty-four hours after the application is made.

The judge may, interrupting the time limit above referred, request expansion or clarification of the terms of the application, as long as this is necessary to decide on the performance of any of the requirements.

The judicial decision authorising the measure will, at least, specify the following facts:

a. The punishable act subject to investigation and its judicial classification, with a statement of the prima facie evidence grounding the measure.
b. The identity of those under investigation and any other affected by the measure, if known.
c. The extent of the interception measure, specifying its scope and the grounds in relation to compliance with the guiding principles provided for in article 588 a. i.
d. The investigation unit of the Judiciary Police that will be in charge of the intervention.
e. The duration of the measure.
f. The manner and frequency with which the applicant will report to the judge on the results of the measure.
g. The purpose of the measure.

h. The person in charge who will carry out the measure, if known, with express mention of the duty to collaborate and be sworn to secrecy, as appropriate, with a warning on committing the offence of disobedience.

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

Article 588 sexies c, in its first two paragraphs, addresses the analysis of four aspects that are essential to the effectiveness of records of mass storage devices: (i) the need for the court decision to specify the terms and scope of the record, (ii) the possibility of making copies of computer data, (iii) the need to set conditions to ensure the preservation and integrity of the data, and (iv) the advisability of avoiding the seizure of storage media, with some exceptions.

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?*

The basic principle under which these devices can be seized, read, accessed, and/or analysed is based on a judicial authorization and only under the above mention circumstances, they can be trespassed upon. This, because the legal system is protecting fundamental rights recognised in the Spanish Constitution.

So, as stated in the previous answer the limits are the rights recognised in article 18 of the constitution regarding the Right to honour, privacy and own image.

(i) Art. 18.1: *The right to honour, personal and family privacy and own image is guaranteed.*

(ii) Art 18.3: *"The secrecy of communications and, in particular, of postal, telegraphic and telephone communications, is guaranteed, except in the event of a court order.*

(iii) Art. 18.4: *"The law shall limit the use of computer science in order to guarantee the honour and personal and family privacy of citizens and the full exercise of their rights.*

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

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

If you fail to provide a judicial authorisation, and you can't seize the device under the urgent cases circumstances, it could only be seized under the consent of the owner, without prejudice of the limits stated before, regarding individuals who are arrested, under investigation, or prosecuted.

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

There is, and it is stated in the Constitution the duty to collaborate with judges (art. 118). Accordingly, article 588.sexies.c and article 19 of the Budapest Convention call on the States Parties to adopt such legislative and other measures as may be necessary to empower their competent authorities to order any person who has knowledge of how computers system works to supply all necessary information.

The duty of cooperation imposed is, however, subject to certain limits in the LECrim. It is possible to speak of a subject limitation, which would restrict individuals from whom collaboration may be demanded, and an objective limitation, which exempts from the duty when collaboration is particularly burdensome.

As for the subject limitation, **the provision expressly excludes from the duty to collaborate the person investigated or prosecuted,** his closest relatives and those who, in accordance with the provisions of art. 416.2 LECrim, are exempted from the obligation to declare by virtue of professional secrecy. The dispensation granted to the investigated or accused person is a logical consequence of the scope of his own right of defence and the power derived from it, which allows him not to testify against himself.

So, no individual can be force to unblock the device without the proper judicial authorisation. Specially, we will need to be extremely careful when we are dealing with a person who has been arrested, is under investigation or prosecuted because, we cannot get consent without the

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

presence of an attorney and we cannot invoke the duty to collaborate, since the prosecuted has his own right of defence.

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

Not necessary if the proper judicial authorisation has been given.

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

There is nothing against it. However, since, we are talking about already seized devices, it can be limited by the judge either in the prior judicial authorization or in the subsequent validation.

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

If we speak to the proportionality of the measure, in accordance with the general criteria established in the LECrim, to assess the case in question, the judge will have to state the legal framework that justified the sacrifice of the rights and interests of the person concerned.

Thus, for example, in cases of particularly serious offences, where the life of a person or public security is at stake (as would be the case with terrorist offences), the particular interests of the individual must normally be ceded. On the other hand, in the case of minor offences or where the data which the search may provide to the investigation are not particularly decisive, the interests of the individuals must be assessed more strongly. For the above purposes, in Spain, those offences that are punishable by a prison term of more than 5 years are considered grave offences.

For the same reason, we can also mention the Law, 25/2007, of 18 October, on the conservation of data relating to electronic communications and public communications networks, which aims to regulate the obligation of operators to retain data generated or processed in the context of the provision of electronic communications services or public communications networks, as well as the duty to transfer such data to authorised agents whenever they are required to do so by means of the corresponding judicial authorisation for the purpose of detecting, investigating

and prosecuting grave offences under the Criminal Code or special criminal laws. So, it can be understood, that if we are before minor offences the rights to privacy and own image may be protected.

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

Access to external computer systems may raise issues of jurisdiction. Indeed, the absence of borders on the Internet, coupled with the lower costs of service in certain countries, will often mean that data storage servers are physically located outside the territory in which the judge authorising the registration exercises jurisdiction (or even the place where they are located is unknown). In these cases, if one starts from a traditional conception of the limits of jurisdiction based on territorial criteria, it might seem more correct to resort to international judicial cooperation mechanisms to obtain such data, which, however, would be absolutely incompatible with the speed required for this type of investigation.

Furthermore, in many cases, either the location of the data is unknown (offshoring) or the data are fragmented in servers located in various territories or their location in one or another place is beyond the control of the data subject and depends exclusively on the technical or operational convenience of the storage service provider that changes the location according to its own needs. Therefore, making the collection of data conditional on the location of the data would lead to the failure of many investigations simply because the exact location of the data is unknown, thus rendering the international cooperation measures adopted ineffective.

In view of this perspective, the Spanish legislator has decisively opted for the legality of access with simple judicial authorisation, even in cases where the data are located outside Spain. This is evident from the literal interpretation of the legal regulation, and even more so, if it is

compared with the immediate precedent, article 350.4 of the Proposed Criminal Procedure Act, which limited access to data stored in computer systems located in Spanish territory, referring to international judicial cooperation in the rest of the cases. This provision followed the criteria of art. 19.2 of the Convention on Cybercrime that, in its Explanatory Report, expressly stated that the rule did not allow the registration of systems located outside the national borders, referring also to international judicial cooperation for these cases.

The approach now being taken, however, is to consider telematic storage repositories as a further part of the system being recorded. What matters is not where the data are physically located, but where they are accessed from.

So, it can be stated that if the owner access these data from Spain and exercises his rights over them from Spain and in accordance with Spanish law, it can be stated that when they access it is done from Spain and in accordance with Spanish law provided, of course, that, as has been pointed out, one can speak of legal access. Just as it would be illogical to consider that the holder of child pornography cannot be prosecuted in Spain if the files are located on servers located abroad, it would be illogical to consider that the Spanish judge cannot access data from a computer system located in Spain because the specific data being accessed is on a server located abroad.

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

Please view answer 13 and 25.

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?*

As long as there is proper judicial authorization.

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?*

It must be carried out by judicial authorization, or in its absence, with the consent of the owner of the device.

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

If we speak to the proportionality of the measure, in accordance with the general criteria established in the LECrim, to assess the case in question, the judge will have to state the legal framework that justified the sacrifice of the rights and interests of the person concerned. Thus, for example, in cases of particularly serious offences, where the life of a person or public security is at stake (as would be the case with terrorist offences), the particular interests of the individual must normally be ceded. On the other hand, in the case of minor offences or where the data which the search may provide to the investigation are not particularly decisive, the interests of the individuals must be assessed more strongly. For the above purposes, in Spain, those offences that are punishable by a prison term of more than 5 years are considered grave offences.

For the same reason, we can also mention the Law, 25/2007, of 18 October, on the conservation of data relating to electronic communications and public communications networks, which aims to regulate the obligation of operators to retain data generated or processed in the context of the provision of electronic communications services or public communications networks, as well as the duty to transfer such data to authorised agents whenever they are required to do so by means of the corresponding judicial authorisation for the purpose of detecting, investigating and prosecuting grave offences under the Criminal Code or special criminal laws. So, it can be understood, that if we are before minor offences the rights to privacy and own image may be protected.

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.*

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

Yes, that situation will always lead to the inadmissibility in court of the evidence.

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

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

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

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

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

Any such measure or modification must be authorized by a judge

***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.

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

There is no specific regulation against the use of a specific mobile forensic tools, or AI technology. However, the use of mobile forensic evidence, regulated in the LECrim (Art 588) must be respected by all means.

***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

To the effects of mobile forensics, please view question 13.

***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?*

When the effectiveness of a Spanish criminal decision requires the practice of procedural actions in another Member State of the European Union, in the case of an instrument of mutual recognition regulated by this Law, the competent Spanish judicial authority shall document it on the mandatory form or certificate, which it shall transmit to the competent authority of the other Member State for its execution.

The "issuing authorities" are the Judges and Courts that are hearing the criminal proceedings in which the facts are being investigated and have admitted the evidence, and the Prosecutors in the proceedings that they conduct, when the measure in question does not restrict fundamental rights.

And the "executing authority" of the IEO is the Public Prosecutor's Office, which will receive and register it, and then either take it over for recognition or execution, or, if it contains measures limiting fundamental rights or if the issuing authority so requires, refer it to the competent court or tribunal.

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

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.

Mutual legal assistance mechanisms are gradually being replaced by mutual recognition instruments. However, there is still agreement between EU countries: the convention on mutual assistance in criminal matters strengthens cooperation between judicial, police and customs authorities.

Each country designates a central authority, usually the two Departments of Justice, for direct communication. The treaties include the power to summon witnesses, to compel the production of documents and other actual evidence, to issue search warrants and to give notice of proceedings. Generally, the remedies offered by treaties are available only to prosecutors. The defence must normally proceed with the methods of obtaining evidence in criminal matters under the laws of the host country, which usually consist of letters rogatory

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.

There are no institutionalised cooperation mechanisms as such, but it should be noted that the aforementioned duty of cooperation, as set out in the Constitution and mentioned in the questions 9 and 21, would come into play here. For the same reason, we would also have to take into account the Law, 25/2007, of 18 October, on the conservation of data relating to electronic communications and public communications networks, developed in the questions 14 and 29.

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:*

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

- *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.

In order to have access to the information and data collected on mobile forensics that is being investigated, an enabling court decision will be required, in accordance with Article 588 septies a.2. This must specify the purpose of the registration, its scope, the form of access to the system (mentioning the technique used to access the passwords or device codes), the agents authorised to carry out the measure, the authorisation, where appropriate, to make copies and keep them, as well as the measures to secure the registered data. All these mentions will, of course, be added to the content of any court order authorising a technological research measure under Article 588a(c). Notwithstanding the foregoing, the fact that research is authorised by carrying out searches on all the data stored on a device does not mean that the privacy of all such data will be accessed.

In addition to specifying the scope of the search and deciding whether or not to make copies, the court decision must also set out the necessary conditions for ensuring the integrity of the data and the guarantees for its preservation in order to make it possible, if necessary, to have an expert opinion.

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

Although the practice of making copies is common in mobile forensics, a court decision agreeing to the measure will always be required. In order to guarantee the integrity of the evidence, the analysis and recording will be carried out on the copies obtained from the device.

The practice of making copies from mass storage devices can be done in two ways. By cloning or dumping, which consists of making a mirror or bit-by-bit copy of the original information, or by making a logical copy, i.e. a selective copy of certain folders or files. In the first case, the image obtained with the copy will be identical to the original and must be digitally signed through a hash function, which will guarantee the identity of the computer data between those existing in the copy and the original. In the case of logical copies, without prejudice to the fact that a digital signature is also possible by means of the hash function, it would be advisable to have it carried out in the presence of the Legal Counsel of the Administration of Justice in order to provide greater guarantees for the selection of files to be copied.

Although the intervention of the Legal Counsel of the Administration of Justice is not necessary during the copying process. Sometimes it will be necessary to guarantee the identity and integrity of the evidence by issuing a report at the moment of unsealing the device and beginning the cloning. However, in the case of logical copies, the best way to guarantee what is being copied, how it is being copied and the integrity of the copy will be to do so in the presence and under the faith of the Counsel for the Administration of Justice. Article 476 of the Criminal Procedure Act recognizes the possibility of appointing an expert to witness the act, but, nevertheless, "this presence is not a prerequisite for the validity of the act"

In order to guarantee the identity of the seized devices, the Legal Counsel of the Administration of Justice must mention in the record of the search the reason why the device was seized. In order to guarantee the integrity of the devices, it will be necessary for them to be properly sealed and made available to the courts at the time of their seizure. Any subsequent opening of the seal, as would be necessary to carry out the cloning of the device,

must be done under the faith of the Counsel for the Administration of Justice; once the cloning has been carried out, the device must be resealed. Notwithstanding the above, in cases where the device is not seized, leaving it in the possession of the person under investigation, two copies must be made.

Section 3: Admissibility of evidence before court

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

There are not specific guidelines, however and to present a reliable mobile forensic with all the guarantees, a digital evidence in a judicial procedure is through the practice of an expert evidence carried out by a collegiate computer expert.

The expert will use both hardware and software tools -own and free, depending on the needs of the case- and, if this professional considers it to be necessary, a notary who will attest to the cloning or dumping of the evidence related to the case and, if appropriate, to the elevation to a public document of the hash obtained for each of said evidence. The hash is the only guarantee of maintaining the chain of custody over the evidence.

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

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.*

The evidential effectiveness of the evidence will depend on the means used for its contribution and on the evaluation that the judge will make jointly of the evidence taken in the process. The LECrim does not expressly mention the evaluation of the evidence by means of electronic documents in the criminal process. Therefore, the only article of application would be the generic article 741.1 of the Criminal Procedure Act, which establishes the principle of free

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

evaluation of the evidence. Therefore, the LEC (Civil Procedure Acta) can be applied in a supplementary manner when evaluating electronic evidence in criminal proceedings.

In legal evidence, the law indicates in advance to the judge the degree of effectiveness that he must attribute to a certain means of evidence. On the other hand, in the system of free evidence, it is the judge who evaluates according to the rules of rational criteria, which does not mean that the evaluation is according to the total discretion or arbitrariness of the judge, but rather that the criteria he uses for said evaluation must be motivated in the sentence.

Taking into account that the criteria used in its evaluation is the system of free assessment, since according to article 384.3 LEC, which is applicable to elements that can file, know or reproduce relevant data for the process, it establishes that "the tribunal will evaluate the instruments referred to in section one of this article in accordance with the rules of healthy criticism applicable to them according to their nature". Recalling that as mentioned above, this article is of subsidiary application to processes in all jurisdictions (art. 4 LEC), given that there is no specific precept on the evaluation of electronic evidence in criminal, labour or contentious-administrative procedural law.

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

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?*

If an offence against fundamental rights is committed in the evidence collection, the evidence will be invalid and ineffective. When an evidence is considered illicit because it violates a fundamental right, its invalidity and loss of efficacy not only affects the evidence that was specifically obtained illicitly, but it will affect the whole of the criminal evidence, that is, it will derive in the rest of the evidence that would have been obtained from it, these being affected or contaminated by the illegality in the obtaining of the evidence from which they came

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

(doctrine of the fruits of the poisoned tree of the Supreme Court of the United States). Based on the above, such evidence shall be considered null and void.

If the evidence has been obtained omitting the provisions of the LECrim or the LEC but without violating a fundamental right, the above would not apply, these would still be illegally obtained evidence, but unlike the case in which fundamental rights are violated, these would not have to be excluded from the process.

Those that were independent of this and those that would have remained unchanged regardless of the infringement that led to the invalidation would not be affected.

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

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?*

View answer to question number 13

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

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.*

If any suspicions arise about the authenticity and/or integrity of the data it is very likely that the judge will end up denying the effectiveness of the electronic evidence.

In his assessment, the judge must take into account the position of each of the parties in relation to the electronic evidence provided, especially if the opposing party rejects (challenge) its validity.

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

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

***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.

Please, view answer to question 48.

***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.*

- **STS of 19 May 2015, Appeal 2387/2014**

It pronounces on the evidential value of communications and instant messaging media, as well as on the need for expert evidence and the burden of proof.

- **STS, of 4 December 2015, Appeal 10447/2015**

Right to Privacy and Secrecy of Communications. This ruling quotes numerous case-law of the Constitutional Court and analyses the right to privacy and its relationship with the secrecy of communications, in its relation to the use of computers and electronic communications in general. Invoking STC 173/2011, 7 November, which among other things states:

> *"On that occasion the Constitutional Court already warned of the meaning of the rights that converge in the use of a computer, as an instrument for navigating the Internet and as a means to make telematic communications a reality: "... if there is no doubt that personal data relating to an individual person, as referred to above, are within the scope of constitutionally protected privacy, even less so can there be any doubt that the accumulation of information stored by its holder on a personal computer, among other data on his private and professional life (in the form of documents, folders, photographs, videos, etc.), is a violation of the right to privacy.) - so that its functions could be compared to those of an electronic diary - not only forms part of this same area, but also through its observation by others, aspects of the most intimate sphere of human beings can be discovered. It is clear that when the holder surfs the Internet, participates in conversation forums or social*

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

networks, downloads files or documents, carries out e-commerce operations, is part of news groups, among other possibilities, he is revealing data about his personality, which can affect the deepest core of his intimacy by referring to ideologies, religious beliefs, personal hobbies, health information, sexual orientations, etc. Perhaps, these data reflected in a personal computer can be labelled as irrelevant or light if considered in isolation, but if analysed as a whole, once conveniently intermingled, there is no doubt that they all form a highly descriptive profile of the personality of their owner, which must be protected against the intrusion of third parties or public authorities, as they concern, ultimately, the same peculiarity or individuality of the person. In addition, the computer is a useful tool for the transmission or reception of e-mails, which may affect not only the right to confidentiality of communications under Article 18(3) EC (since there is no doubt that the use of this procedure involves an act of communication), but also the right to personal privacy (Article 18(1) EC), in so far as those e-mails or mails, whether written or already read by the addressee, are stored in the memory of the computer used. It is therefore necessary to establish a series of guarantees against the risks that exist for public rights and freedoms, in particular personal privacy, due to the improper use of information technology as well as new information technologies.

It also highlighted the possibility that this right may be ceded in the presence of other constitutionally protectable interests, in view of the non-limited or absolute nature of fundamental rights, so that the right to personal privacy, like any other right, may be subject to restrictions (SSTC 98/2000, 10 April, FJ 5 ; 156/2001, 2 July, FJ 4 ; 70/2009, 23 March, FJ 3). Thus, although Article 18.1 EC does not expressly provide for the possibility of a legitimate sacrifice of the right to privacy - unlike what occurs in other cases, such as with respect to the rights recognized in Articles 18.2 and 3 EC -, its scope of protection may be ceded in those cases in which the existence of a constitutionally prevailing interest is found to be in conflict with the individual's interest in maintaining the privacy of certain information".

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

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

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

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

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

Please, view answer to question 48.

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?*

As indicated in the STS, of 4 December 2015, Appeal 10447/2015, there may be some collision between the two rights. However, the possibility exists that this right may be ceded in the presence of other constitutionally protectable interests, given the unrestricted or absolute nature of fundamental rights, so that the right to personal privacy, like any other right, may be restricted. In this same sense, the Constitutional Court, weighing up both rights, established in its Judgement 292/2000, of 30 November, that the right to data protection is not unlimited.

Therefore, the judge, taking into account the circumstances of each case, as well as the applicable legislation and jurisprudence, must assess whether or not it should be admitted.

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

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.

- **STS of 16 June 2014, regarding the admissibility of evidence, that may collide with fundamental rights.**

"...resulting, to this effect, in the authorization and control that only the judge can dispense in our system, even according to labour legislation, which at least apparently follows the same criterion of

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

clear judicial vocation (see art. 76.4, in relation to 90.2 and 4 of Law 36/2011, of October 10, regulating social jurisdiction, in whose concrete interpretation and scope it is not our place to enter here).

Consequently, it must be made very clear that in the area of criminal procedure, which is our responsibility, in order to give value and evidentiary effectiveness to the result of the test consisting of the intervention of communications protected by the right enshrined in Article 18. 3 of the Constitution, it will always requires the authorization and judicial intervention, in the terms and with the requirements and contents that have been so widely elaborated in a multitude of Resolutions by this Chamber, starting with the important Order of 18 June 1992 ("Naseiro" case), whatever the circumstances or persons, police officers, businessmen, etc., that such interferences are carried out.

On the other hand, it is obvious to remember that it will operate only for what strictly constitutes this "secrecy of communications". This means that the so-called "traffic data" or even the possible use of computer equipment to access other services on the network such as web pages, etc., are excluded from messages which, once received and opened by the recipient, are no longer part of the communication itself, as opposed to those governed by different rules such as those on data protection and conservation (Article 18(4) EC) or on documentary privacy in the generic sense and without the absolute requirement of judicial intervention (Article 18(1) EC).''

- **STS 342/2013, 17 April, in relation to the legitimacy of access by public authorities to electronic devices**

"... access by the public authorities to the contents of the computer of an accused person is not legitimised by a unilateral act of the State's security forces. The computer and, in general, the mass storage devices, are more than a piece of evidence that, once seized, is exposed in its entirety to the control of the investigators. The content of this type of device cannot be degraded to the simple condition of being a recipient of a series of data with a greater or lesser relationship to the right to privacy of its user. It is true that technical data and personal data subject to constitutional protection in the field of privacy and data protection coexist in the computer (Article 18.4 of the EC). But its content may also

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

contain - in fact, it normally contains information that is intimately linked to the right to inviolability of communications. Electronic mail and instant messaging management programs are nothing more than technological tools to make the right to free communication between two or more persons a reality in telematic format. It is widely believed that e-mails, once downloaded from the server, read by the recipient and stored in one of the management software's mailboxes, are no longer part of the inviolability of communications. The communication cycle has now come to an end and the information contained in the message is henceforth subject to protection by virtue of its relationship with the area reserved for the right to privacy, the protection of which under the Constitution is obvious, although of a different intensity from that reserved for the right to inviolability of communications. Consequently, access to the contents of any computer by police officers must have the enabling budget of a judicial authorization. This decision must protect the accused against the act of interference by the public authorities. There are many areas of exclusion that must be guaranteed. Not all of them enjoy the same level of safeguards from a constitutional perspective. Hence the importance of guaranteeing those rights always and in any case, in advance, acting as a real enabling budget of a formal nature. The judicial weighting of the reasons that justify, in the framework of a criminal investigation, the sacrifice of the rights of which the computer user is the owner, must be done without losing sight of the multifunctionality of the data stored in that device. Even their legal processing can be made more appropriate if messages, images, documents and, in general, all data revealing the personal, reserved or intimate profile of any defendant are considered in a unitary manner. The fact is that, beyond the fragmented constitutional treatment of each and every one of the rights that converge at the time of the sacrifice, there is a right to the virtual environment itself. This would include, without losing its genuine substance as a manifestation of constitutional rights of nomen iuris, all the information in electronic format that, through the use of new technologies, whether consciously or unconsciously, whether voluntarily or not, is generated by the user, to the point of leaving a trace that can be followed by the public authorities. The need then arises to provide jurisdictional protection against the need of the State to invade, in the tasks of investigation and punishment of crimes, this digital environment".

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

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

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

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

- *Is mobile forensic evidence given a certain probative value?*

  Relating to the evidential value of electronic evidence, we can understand that it must go through three phases:

1. Obtaining the evidence: That it has been obtained in accordance with the established legal framework (already explained in this questionnaire)
2. Incorporation into the process:
    a. Relevance and necessity
    b. Lawfulness
    c. Compliance with procedural requirements (procedural admissibility)
3. Evaluation:
    a. Demand examination of evidence (challenge of the evidence)
    b. Authenticity
    c. Completeness or accuracy

On how to value the evidence, this means giving it the credibility it deserves according to the system established in the law, we can speak of two systems of valuation:

(i) Legal or appraised evidence system: the law indicates in advance the degree of effectiveness that the judge must attribute to a certain means of evidence. For example, documents with the intervention of a notary public.

(ii) Free evidence system: the judge will study the evidence according to his free evaluation, although following the rules of rational criteria. This is the system established for electronic evidence.

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

So, the law does not oblige the judge to consider proven the facts provided in an electronic document (except in the case of electronic public documents). Digital evidence will display its effects to accredit the fact being discussed in court, but its efficacy will be granted by the judge according to the rules of rational criteria.

In this sense, the high technological component of electronic evidence and the importance of scientific knowledge for its evaluation determines the special relevance of expert evidence. It must be taken into account that for the evaluation of electronic evidence the judge must not have any doubts about two features, the authenticity of the origin (its apparent author is its real author) and the integrity of the content (the data have not been altered).

If suspicions arise about the authenticity and/or integrity of the data it is very likely that the judge will end up denying the effectiveness of the electronic evidence.
In his assessment, the judge must take into account the position of each of the parties in relation to the electronic evidence provided, especially if the opposing party rejects (challenge) its validity.

If no challenge is formulated, that is, if the validity of the electronic evidence is not questioned, the judge will tend to consider it to be authentic and exact, and will therefore evaluate it together with the rest of the evidence.

If, however the objection is made, then the judge will consider relevant, on the one hand, the allegations that justify the rejection, and on the other hand, the means of evidence and expert opinions proposed to prove the validity of the evidence.

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

Thus, in reality, the party seeking the validity of the evidence must provide all possible means of proof to strengthen the evidence provided, usually with a computer expert who demonstrates authorship and not manipulation of the data.

- *Are there rules on how to interpret mobile forensic evidence or requirements which must be complied with for the evidence to be considered reliable?*

As stated in the previous answer, the party seeking the validity of the evidence must provide all possible means of proof to strengthen the evidence provided, usually with a computer expert who demonstrates authorship and not manipulation of the data.

And, although the main method of providing electronic evidence is the printing of information on a hard copy and the delivery of electronic data on an electronical support such as a CD, for such evidence to have real reliability, it must have the report of an expert IT witness. As it is a private document, one may choose to incorporate it into a public document, by means of a notarial act. Similarly, the possibility of going to a notary so that he can certify that what is printed corresponds to what is displayed does not guarantee that the evidence has not been manipulated. It would only prove that what is provided contains the same information that the notary has seen on the electronic device.

So, the judge under the principle of rational criteria will asses the electronical evidence.

- *Must such evidence be examined by an expert witness?*

Although we currently have a variety of tools and techniques that allow us to guarantee the truthfulness, origin and accuracy of the information contained in an Electronic document often require the intervention of qualified personnel such as computer experts and notaries in order to make them valid in the context of legal proceedings.

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

When we speak of electronic/mobile forensic evidence, the Supreme Court requires the confirmation of the existence of the fact through computer experts when the evidence is discussed. However, this does not imply that only digital evidence that has been confirmed by computer experts is valid. Therefore, with regard to digital evidence provided by the parties, the provisions of Article 326.1 of the Law of Civil Procedure will apply, which states that "private documents will provide full evidence in the process under the terms of Article 319, when their authenticity is not contested by the party who is harmed".

In STS 224/2017 of 8 March, the High Court states that the possibility of manipulating evidence based on two-way communication by means of instant messaging systems "is part of the reality of things", since such systems allow the creation of accounts freely and guarantee the anonymity of the user. As a result, it is possible to create accounts with a simulated identity and to "simulate a communication in which a single user can relate to himself". Therefore, in criminal proceedings, this type of evidence must be approached with extreme caution.

The aforementioned ruling specifies that the challenge to this type of conversation requires the adoption of certain precautions when it is provided or introduced into the process by means of printed files and "shifts the burden of proof to those who intend to take advantage of its evidential suitability". In the event that such evidence is disputed, and reasonable doubt arises as to its certainty and authenticity, it will be necessary to take expert computer evidence to identify the origin of the communication, the identity of the parties and the authenticity of its content.

Ultimately, authentication is required only in cases where the document is disputed, since, as long as it is not disputed, the document

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

- *If not obligatory, is this a common practice?*

  It is a common practice, since the evidence will be significantly more reliable and will make any challenge made by the counterpart less effective.

- *What are the requirements for experts (experience, independence, training, etc.)?*

  According to article 457 LECrim, experts may or may not be qualified;

  i. Qualified experts are those with an official qualification in a science or art the practice of which is regulated by the Government.
  ii. Unqualified experts are those who, although they do not have an official qualification do have special knowledge or practice of some science or art.

  So, in any case, expertise in the matter of question will be mandatory.

  The Judge will avail of qualified experts in preference to those who are unqualified

- *Is there a centralised management of mobile forensic operations in your jurisdiction to ensure the work is compliant with standards and can be presented in court in a consistent manner?*

  No, that I know of.

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

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

In relation to the assessment and validity of the evidence the Supreme Court in its ruling of May 19, 2015 (STS 300/2015) states:

> *"The evidence of two-way communication through any of the multiple instant messaging systems must be approached with all caution. The possibility of manipulation of the digital files through which this exchange of ideas materializes is part of the reality of things. The anonymity allowed by such systems and the free creation of accounts with a false identity*

make it perfectly possible to appear to be communicating with a single user. Hence, the challenge to the authenticity of any such conversation, when brought to the case through print files, shifts the burden of proof to those who seek to exploit its evidentiary suitability. In such a case, it will be essential to take evidence expert to identify the true origin of the communication, the identity of the parties involved and, finally, the integrity of its contents".

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

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

There is no specific rule regulating the presentation of evidence and imposing a specific process of collection, analysis, interpretation and presentation of digital evidence to be followed for the interpretation and presentation of evidence in court.

This is without prejudice to the rules established in the LECrim in relation to the collection, analysis and presentation of evidence in criminal proceedings, as well as all the other requirements describe in the present document.

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

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

No specific case law has been found to that effect.

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

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

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

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

There are no specific guidelines, or specific guarantees, beyond those already described, regarding the need to prove the veracity of the digital evidence provided.

However, it should be noted that in all processes, including those in which digital evidence is presented, the principles and guarantees set out in the law must be respected. Therefore, those guarantees of obligatory observance must be respected in order to ensure due process, as only the evidence that has been introduced into the trial under the assumptions set forth in the LECrim and other applicable legislation may be taken into consideration in the sentence that ends the process.

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

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

There is no expert training required by law for judges, lawyers and prosecution. So, beyond the requirements for an expert witness indicated in question 48, there aren't more specific requirements.

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

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

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

Not that I know of, however in any case it will be necessary to respect the procedural timeframes established by law and if necessary, by the judge.

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

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

- **Prosecution:** The Public Prosecutor's Office is a necessary party in trials held for public or semi-public crimes (which are prosecuted ex officio by the authorities) in which there has been a complaint from the offended party.

  It must promote the action of Justice in defence of the Law, the rights of citizens and the public interest; it must also ensure the independence of the Courts and seek before them the protection of the social interest.

  Among others, the most important functions of the Public Prosecutor's Office are:

  - To bring criminal and civil actions, regardless of whether there is a private prosecutor; it may also oppose actions brought by others.
  - To watch over fundamental rights, public liberties, compliance with resolutions? etc. when they affect the public and social interest.
  - May intervene in criminal proceedings by requesting the judicial authority to take precautionary measures such as arrest, pre-trial detention, bail, etc.
  - It may visit at any time the detention, prison or internment centres in its respective territory, examine the inmates' files and request any information it deems necessary.
  - In accordance with the provisions of the Act, officials of the Public Prosecutor's Office are obliged to bring all criminal proceedings they consider appropriate, whether or not there is a private prosecutor in the case, except for those which the Criminal Code reserves exclusively for private prosecution, pursuant to article 105 of the Criminal Code.

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

- **Court:** Article 9.3 of the Spanish Constitution (CE) establishes the principle of responsibility of the public authorities and Article 117 CE which determines that Justice emanates from the people and is administered on behalf of the King by Judges and Magistrates who are members of the Judiciary, independent, irremovable, responsible, and subject only to the rule of law. This precept is reproduced in Article 1 of the Organic Law of the Judiciary in which submission to the Constitution is added.

  The use of the freedom and guarantees that the law provides to the judge, in the development of the jurisdictional function, requires a responsible exercise of them before the defendant as a counterpoint to judicial independence.

- **Defendant**: In Spain, from the very moment of arrest, that person has the status of "accused", enjoying all the rights inherent in that status, and must be made aware of this by the police or, where appropriate, by the investigating judge. These rights are; (i) right to defence and legal assistance, (ii) right to be informed of the charge against him, and (iii) the right to remain silent and not to testify against himself. Once the person in question have the formal status of "accused", he or she can take cognizance of what has been done and urge what is appropriate to his right, being empowered to ask for whatever actions he deems appropriate.

- **Witness:**
  - All those residing in Spanish territory, whether nationals or foreigners, who are not disabled, **will be obliged to attend the judicial appeal to declare what they know** about what they were asked if they are summoned to do so with the formalities prescribed by law.
  - The relatives of the defendant in direct ascending and descending lines, his spouse or person united by a de facto relationship analogous to marriage, his blood or uterine siblings and blood relatives up to the second civil degree, are exempt from the obligation to declare.

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

- The witness's statement must be recorded in the proceedings in the language used by the witness and then translated into Spanish. (arts. 440 and 441 of the Criminal Procedure Act), in which case the court must provide them with an interpreter who will be sworn or promised.

- **Victim:** The rights of victims are set out in Law 4/2015:
  - Right to understand and be understood
  - Right to information from the first contact with the competent authorities
  - Rights of the victim as a complainant
  - Right to receive information about the criminal case
  - The right to a period of reflection to guarantee the rights of the victim
  - The right to translation and interpretation
  - Right of access to assistance and support services

5.1 The Prosecution

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

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

Please, view answer to question 48

5.2 The Court

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

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

As indicated throughout the questionnaire, there are no specific controls in the Spanish law with respect to the valuation, means of acquisition and analysis of digital evidence.

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

This is without prejudice to the fact that the acquisition of the test must be carried out legitimately and as described in section 1 of the questionnaire. For the same reason, and in relation to the assessment and analysis of the evidence, within the freedom that the judge may have, he must always do so under the principle of rational criteria and in accordance to case law that may apply, such as the STS 300/2015, Supreme Court in its ruling of May 19, 2015, mentioned in section 4.

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

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

View answer above (question 58), and also related to answers in section 4.

5.3 The defendant and defender

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

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

Article 118 sets out the rights of the defendant in a criminal case, including among others, the right to be informed about the acts ascribed to them and any relevant change in the subject of the investigation and the grounds on which the accusation was based (information will be given with a sufficient amount of detail to enable effective exercise of the right to a defence). And also, the right to examine the proceedings sufficiently in advance to safeguard the right to a defence and, at any event, prior to their statement being taken.

Moreover, Article 234 of Organic Law 6/2018 of the Judicial Power states that the lawyers of the Administration of Justice and competent officials of the Judicial Office will provide interested parties with any information they request on the status of judicial proceedings, which they may examine and learn about, unless they are or have been declared secret or reserved in accordance with the law.

There have been some conflicts, as some judicial offices understood that providing copies could violate data protection law. In this context, we can understand that the right to effective judicial protection is above the right to data protection. In fact, and in view of the conflict of rights arising between data protection and effective judicial protection, the Constitutional Court, weighing both rights, established in its Ruling 292/2000, of 30 November, that the right to data protection is not unlimited.

5.4 Witnesses

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

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

There is a specific Organic Law 19/1994, of 23 December, on the protection of witnesses and experts in criminal cases. The system in place gives the judge or court a rational assessment of the degree of risk or danger and the application of all or some of the legal protection measures he or she considers necessary, after weighing up, in the light of the proceedings, the various constitutionally protected legal assets; measures which, within the framework of the right to defence, will be subject to appeal for both purposes.

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

Regarding the capability in respect to mobile forensics, it will depend on the facts the witness knows and will testify to. In any case, and if he is testifying at an expert or technical level, it will be necessary for him to justify his technical knowledge

5.5 The Victim

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

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

In Spain, there is a law that establishes the legal status of the victim of the crime, Law 4/2015, of April 27th, on the Statute of the Victim of the Crime. Public authorities, offers the widest possible response, not only legal but also social, to victims, not only to repair the damage in the framework of criminal proceedings, but also to minimize other traumatic effects on morale that their condition may generate, all regardless of their procedural situation.

All victims shall have the right to protection, information, support, assistance and care, as well as to active participation in the criminal process and to be treated in a respectful, professional, individualized and non-discriminatory manner from their first contact with the authorities or officials. Regulating their rights to understand and be understood, to information, to obtain a copy of the complaint, translation, free legal assistance, etc.

As parties to the legal process, they may use any lawful and legitimate means of evidence at their disposal, including mobile forensics.

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

Section 6: Comments

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

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

After the reform operated in Spain, by Organic Law 13/2015 of October 5, on the modification of the Law on Criminal Procedure for the strengthening of procedural guarantees and the regulation of technological research measures, the regulation for the registration of computer devices and systems is introduced.

In this way, our legal system gives room to the leading role acquired by computer science in recent years, and how it has affected the way in which many criminal behaviours are developed that either fall directly on computer devices or systems, thus causing the birth of new forms of crime, or use computer science as a privileged means or instrument for their development. It is precisely for this reason that in recent years the use of information technology has also proved to be crucial to the prosecution of crime.

All the regulation that is now established will always be presided over by the common provisions of general application to all technological investigation proceedings that are contained in Chapter IV of Title VIII of Book II LECrim.

Traditionally, the jurisprudential doctrine has considered that two different fundamental rights may be compromised in the registration of computer devices or systems. In general, it was understood that the privacy of the user of the device was affected, since all the data that can be stored on the device (in the form of documents, folders, photographs, videos, etc.) are likely to "affect the deepest core of his or her privacy by referring to ideologies, religious beliefs, personal hobbies, health information, sexual orientations, etc. (STC No.

173/2011, November 7). But, at the same time, limitations to the fundamental right to the secrecy of communications could also arise if the registration of the device (computer or mobile phone, for example) reached stored data that were part of communicative processes.

The solution to the problem was provided by a new jurisprudential doctrine that addressed the problem in a unitary manner, introducing the concept of the "right to the virtual environment" as a single right that covers the protection of the great diversity of data that can be stored in a computer device or system, such as a computer. Therefore, the authorization for the registration of a device or computer system in which access to the entire virtual environment of its user is enabled, will prevent problems arising from the nature of the content that could be found.

- **Applicable Spanish legislation, and references:**
  - Spanish Constitution (CE, Constitución Española)
  - Criminal Procedure Act (LECrim, Ley de Enjuiciamiento Criminal)
  - Civil Procedure Act (LEC, Ley de Enjuiciamiento Civil)
  - Criminal Penal Code
  - Organic Law 6/2018 of the Judicial Power
  - Organic Law 13/2015 of October 5, on the modification of the Law on Criminal Procedure
  - Organic Law 19/1994, of 23 December, on the protection of witnesses and experts in criminal cases
  - Law 4/2015, of April 27th, on the Statute of the Victim of the Crime
  - Law, 25/2007, of 18 October, on the conservation of data relating to electronic communications and public communications networks
  - Ley 3/2018, de 11 de junio, por la que se modifica la Ley 23/2014, de 20 de noviembre, de reconocimiento mutuo de resoluciones penales en la Unión Europea
  - Circular 5/2019 of 6 March from the Public Prosecution Service

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

Please note that any reference indicated as “STS”, refers to a ruling from the Spanish Supreme Court.