formobile@netlaw.bg
Linkedin – Formobile-
Twitter –
www.formobile-

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 –
www.formobile-

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 –
www.formobile-

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

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

formobile@netlaw.bg
Linkedin – Formobile-
Twitter –
www.formobile-

Introductory questions:

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

Answer: Cugia Cuomo & Associati, equity partner.

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

Answer: Rome, Italy.

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

No, there is not a legal definition of "mobile device" in our jurisdiction, in contrast, as example, with the legal definition of "software".

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?*

formobile@netlaw.bg
Linkedin – Formobile-
Twitter –
www.formobile-

5. *Are there any limits to this search (e.g. core area of private life, privacy limits, limits defined by the crime, limits defined by the order/warrant)? If so, how precise are these/must these be defined?*
6. *Is it allowed to use technical tools to bypass security?*
7. *Can information be copied or only read at this stage?*
8. *Is consent of the owner/person in possession of the mobile device necessary?*
9. *Can the owner/person in possession of the mobile device be forced to unlock the device?*
10. *Must the owner/person in possession of the mobile device be informed?*
11. *Who can order a search and what are the formal requirements, if any?*
12. *Does it matter whether this person is the accused or witness/third party or the victim?*
13. *What about data stored in the Cloud, what is the procedure to access/read this data if it is known or suspected to reside outside your jurisdiction? Is international cooperation like the European Investigation Order (hereinafter: EIO) or Mutual Legal Assistance Treaties (hereinafter: MLAT) the only route or do other options exist? Please elaborate.*
14. *Does any of the foregoing depend on the type of crime involved (e.g. terrorism, child pornography etc.)?*
15. *Does not following the applicable rules always lead to inadmissibility in court of the evidence in this scenario? If not, please elaborate on exceptions and relevant conditions.*

<u>*Mobile device seized*</u>

16. *Can the mobile device (e.g. a smartphone) be seized?*
17. *What are the conditions for this, who can order it and what are the formal requirements?*
18. *If seized, can the mobile device always be searched, information copied etc?*
19. *Are there any limits to this search (e.g. core area of private life, privacy limits, limits defined by the crime, limits defined by the order/warrant)? If so, how precise are these/must these be defined?*
20. *Is consent of the owner/person in possession of the mobile device ever a relevant element?*

formobile@netlaw.bg
Linkedin – Formobile-
Twitter –
www.formobile-

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

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

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

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

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

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

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

28. *How is the access to data kept by a Service Provider related to the device regulated? Is it performed upon a Court order, or also through other means?*

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

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

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

formobile@netlaw.bg
Linkedin – Formobile-
Twitter –
www.formobile-

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:

Mobile device not seized

Any mobile device or smartphone that has not been seized could be reached or grabbed by the criminal police, if classified as evidence.

On the basis of art. 244 c.p.p. (Italian Criminal Procedure Code) with a motivated decree of the Judge for preliminary investigations can be ordered the inspection of persons, sites or things, in the event that it is necessary ascertain traces and other material effects of the offence, ordering technical operations "also in relation with computer or electronic systems, implementing appropriate technical measures to ensure data retention and to prevent data alteration". Through a motivated decree of the Judge for preliminary investigation, on the basis of art. 247 co.1-bis c.p.p. may be ordered the search "when there are reasonable suspects for believing that data, information, computer programs or traces still relevant to the offence are located in a computer or electronic system, although protected by security measures"; the operations are always implemented "adopting technical measures to ensure data retention and to prevent data alteration".

Moreover, on the basis of art. 352 co. 1-bis c.p.p., can be ordered the search of computer or technological systems, although protected by security measures, if the Judicial Police "has reason to believe that in these systems are hidden data, information, software or traces still relevant to the offence that can be deleted" in caso of:

- flagrante delicto;
- execution of a restraining order;

- execution of a custody order of the suspect or convict, in the case of offences involving mandatory arrest in flagrante delicto on the basis of art. 380 c.p.p.;
- detention of the suspect.

In such cases the Judicial Police adopts all the technical measures to ensure data retention and to avoid data alteration. In contrast with other forms of search, there is not a prior authorization decree issued by the Judge. Indeed, the Judicial Police, for particular and specific purposes that would not allow the issuing of a search decree, perform investigative activities sending the case file within 48 hours to the local prosecutor, including the record of operations; if the legal conditions are satisfied, the prosecutor validate the search within 48 hours following the sending.

During search operations of mobile devices, the Judicial Police employs Computer Forensics operating on devices, particularly:

- Shall identify and isolate the computer systems on the site being searched;
- Shall identify and isolate online accounts;
- Shall require login credentials, lock codes, PIN and password and proceed to change;
- Shall require the presence of encrypted data and its decryption password.

Moreover, Computer Forensics proceed to acquire all data present on mobile devices, creating backups and duplicating it on another digital support.

In event of refusal of the suspect to provide login credentials, Computer Forensics can operate in download or fastboot mode (Android system), or DFU mode (iOS system), in order to bypass the lock codes of mobile devices, if any.

After duplicating data, Computer Forensics verify that the duplicates correspond to the original and return the intact and functioning mobile devices.

Data could be accessed by legal authorities for the purposes of the criminal proceeding, and also could be consulted by the parties to the proceeding, pursuant to the Italian criminal procedure code.

Searches on mobile devices, it should be noted, can be ordered solely on mobiles of ownership, or otherwise used by suspects, does not depend upon offence type for which investigations are being carried out.

An issue of particular interest relates to cloud data capture mode, that are located outside Italian territory. In order to comprehend the issue, it seems useful to analyse the case law of the Courts concerning encrypted data recovered from Blackberry chats.

Indeed, in this case, the conversations happen through chat messaging apps, in pin to pin system, which codes are hold by Canadian corporate RIM (Research in Motion).

In investigative and judicial practice, the problem of international letters rogatory has been solved by using the "routing" technique, avoiding to request an international letter rogatory.

The prevailing case law, verily, does not consider necessary to request an international letter rogatory, because it can be used, without needing a letter rogatory, the results of interception of communications by chat in pin to pin system, managed by server located in foreign territory, but which data are recorded in Italian territory through systems setted at Public Prosecutor's offices.

The same prevailing case law, again, has found irrelevant that pin to pin interconnections have taken place through a Canadian server, because the flow of information was originally turned from the RIM's head office straight to Public Prosecutor's centralised IT system, by a passage ("routering") from a Data Manager to legal authorities, within the Italian territory, for which it would be necessary any international letter rogatory, thus justifying that RIM's Italian corporate branch routered the flow of information to legal authorities, and so data routering and its recording process took place, peacefully, in Italy.

Although we do not ignore the circumstance that the Italian Supreme Court many times has been called upon to rule on pin to pin chats tapping, for which considered that the interceptions activities are respectful of Italian crime law and they do not need any international letter rogatory, it is necessary to point out our dissenting opinion.

Indeed, although in Italy it happens a plain e simple acquisition of data, it is also true that these data have been decrypted only because of a third party, operating abroad, that in its territory decrypts data and forward to the relevant legal authorities, without forwarding the source codes used for decrypting activities that, in fact, remain in foreign territory and sole property of RIM, without the relevant legal authority having checked the validity of the source codes.

Moreover, it is appropriate to specify some steps that characterize the chat pin to pin between Blackberry devices that allows, as known, to holders of such devices to exchange written communications through an IT system created by RIM (in addition, it is worth noting that RIM has its registered office in Canada, and this country solely owns the decrypting codes and performs data processing operations).

Very briefly, the subject who sends a message to another user starts the following sequence: ***a)*** the message is encrypted by the smartphone, ***b)*** the message is sent to RIM's served allocated in Canada, that operates a first task of data processing and encryption, ***c)*** from there, the message is re-sent to the smartphone receiver, that ***d)*** unpacks the message and makes it visible through the decryption keys owned by RIM's head office in Canada.

Through such technology, then, it is not possible to intercept the chats using phone companies' traditional channels, because RIM's data passing through it can not be decrypted without RIM's necessary cooperation, not being telephone records, but telematic flows, as encrypted files.

So, the problem is similar to that which arose with Skype conversations (in investigative practice it was solved, or rather obviated, through the installation of a spy software into the intercepted device, capable to immediately capture and record any conversations, before they are encrypted by the sender, or after being decrypted by the receiver, so obviating to the problem on decrypting code acquisition, solely hold by the software house in foreign territory).

Instead, in this case the Judicial Police, while being able to install a spy software on suspect's phones, prefers to request to the company manufacturer (Blackberry) the acquisition of data.

So, what comes to relief is the execution of the interception of telematic flows, also subject to the same rules that regulate telephone tapping. The sticking point is, therefore, to establish where e how the collection operations can be performed, and to whom may be delegated.

On the basis of art. 268 co. 3 cp.p., these operations must be performed at Public Prosecutor's offices. However, in case of interception of telematic communications, the Public Prosecutor can order the use of IT privately-owned facility, on the basis of art. 268 co. 3 bis c.p.p. This discipline is one of the "guarantees established by law" referred to in art. 15 Italian Constitution, whereas,

therefore, it must guarantee direct control of the investigating Prosecutor over such operations that, inevitably, have effect on assets of constitutional rank.

As mentioned, in order to intercept Blackberry devices (particularly, applications using pin to pin system) the legal authorities request to RIM's Italian corporate branch (RIM Italia s.r.l.) that, however, is obliged in its turn to forward the request to the Canadian head office, solely owner of the server through which pass the chats "pin to pin" and solely owner of decrypting keys. Only this legal entity, thus, performs in foreign territory, in complete autonomy, the collection of telematic flows, decrypting data, and transmits the processed data through the Italian branch, merely facilitator between RIM and the legal authorities, that have not controlled this data processing.

It is quite clear that this procedure breach Italian criminal legislation (art. 268 co. 3 and 3 bis c.p.p.). Moreover, prevailing law has always distinguished the concept of installation of plants at Public Prosecutor's offices, from that of property of the same plants, especially "the obligation to use "installed" plants at the Public Prosecutor's Office, or public service or "supplied" to the police resulting from this normative forecast, *,by no means excludes the use* use of IT privately-owned facility *and does not affect the legal instrument (purchase, loan, lease or other) through which the Public Prosecutor or Judicial Police obtain such equipment, but requires only that they be installed in the judicial offices or are in the possession of the police*" (Cass. Pen, Sez. I, 19 dec. 2014, n. 3137).

Moreover, it is important that the collecting, recording and decrypting activities of the messages take place at Public Prosecutor's offices, because it would consent a direct control by the Public Prosecutor over operations, allowing the use of equipment located outside only when audio surveillance interceptions are to be carried out (Cass., sez. VI, 25 June 2002, n. 1281, Barilari, in Riv. pen., 2004, p. 137).

So, art. 268 c.p.p., contrary to what is claimed by prevailing case law, does not accept that the activities of collection can be carried out with facilities allocated to private entities, then we can not share the opinion of the prevailing law that the code rule would be respected, because "the passage of the data (routing) from the Blackberry's Italian corporate branch to the legal authorities occurred on national territory [...] and on Italian territory [...] data recording operations have been

carried out and, therefore, lawfully omitted the use of the international mutual legal assistance procedure and fully usable are the results of interceptions (original magnetic media related to interceptions were last were last forwarded to the Public Prosecutor's Office of the Republic of Palermo at whose Offices they are kept with possibility to the parties of access [...] ".

In fact, the evidence is not formed by a collection activity, but through the decryption of telematic flows established abroad, at privately-owned facilities and, thus, without this activity being carried out under the direct control of the Judicial Authority (in this case, by the Public Prosecutor).

Indeed, in the investigation practice, at the offices of the Public Prosecutor a mere backup activity takes place, from the magnetic support provided by RIM Italia Srl (who in turn received the data processed by the Canadian head office) to the servers used by the Public Prosecutor: it is clear that this activity certainly cannot be lumped in the notion of "recording operation".

The violation of the rules referred to in art. 268, co. 3 and 3 bis c.p.p. inevitably involves the penalty of the unusability of the interceptions carried out and decrypted, using plaints installed at private entities with the additional vulnus resulting from the use of decryption keys solely owned by the private entity (by the way foreign), keys never forwarded to the Public Prosecutor.

Indeed, collective operations of the flows, and the next data decryption, are carried out materially and particularly in Canada by the private entity, within the State in which are physically located RIM's server and are kept the decryption keys: then, it is quite clear that the telematic flows were caught and decrypted abroad. Only as a result of investigative activities at the Canadian headquarters of RIM the source of evidence can be said to be assured (having before the decryption activity a file completely devoid of value and indecipherable), ready to be kept for the next stages of the proceedings, and therefore cannot be in doubt that we are faced with an evidentiary acquisition activity performed abroad.

It is therefore clear that such transactions are in open and wide contrast with art. 268, co. 3 and 3 bis, c.p.p.

Final, it should be noted that this violation "integrates the extremes of pathological unusability" because "it creates a situation of objective uncertainty about the place of objective development of the interception operations, and on the equipment effectively used" (*ex plurimis* Cass. Pen. Sez.

III, 13.05.2014, n. 40209). All acts acquired in violation of art. 729 c.p.p. therefore entail, for express normative prediction, pathological unusability ascertainable, *ex* art. 191 co. 2 c.p.p., ex officio at all levels of the proceedings.

However, it is quite clear that the "routing" technique it is a "*deus ex machina*" useful and necessary to solve the operational aspects which would have been in case of international letter rogatory. Pending a clarification by the European Court of Justice, or by the European legislature, also in relation to the cloud systems the same considerations could be applied, as above. These considerations shall also apply where the mobile device is under seizure.

In the event that the procedures described above for the search of data on mobile devices are not respected, any relevant evidence due to the duplication of data on mobile devices, on the basis of art. 191 c.p.p., are unusable in court. However, such inactivity must be detected by the party or ex officio by the Judge, at all level of the proceedings.

Mobile device seized

A mobile device may be seized:

- probationary (on the basis of art. 253 c.p.p.), where it represents the body of the offence or what is relevant to the offence and is necessary for establishing the facts. It can be ordered at any stage of the proceeding on the initiative of the Public Prosecutor or by Judicial Police delegated, for this purpose, by the same decree that order the seizure. However, whenever there are grounds for suspicion that things could be altered, on the basis of art. 354 co. 2, c.p.p., the Judicial Police on their own initiative carry out the necessary operations, including by seizing the device. If the conditions are met, the Public Prosecutor validates the seizure carried out by the Judicial Police within 48 hours following the request for validation;

- preventive (on the basis of art. 321 c.p.p.), if it represents something pertaining to the crime and the free availability of the same may aggravate or prolong the consequences of the offence itself or facilitate the commission of other crimes. It may also be ordered if confiscation is permitted. It is ordered at all level of the proceedings by the Judge under request of the Public Prosecutor. In the course of preliminary investigations, in cases of absolute urgency, it is ordered by the Public Prosecutor or by a police officer delegated and moreover validated by the Judge under request of the Public Prosecutor.

Concerning the acquisition of data on the device, apply the same considerations as previously noted for the mobile devices not seized but subjected to search. So, the data will be duplicated in a duplicate forensic copy, without any limitation concerning the acquisition of particular types of data and after obtaining the login credentials and always subject to the control by the legal authorities. The mobile device seized, after the duplicate operation, shall be given back to the suspect/defendant. Even then, the seizure shall be ordered solely on a owned device or however used by the suspect/defendant and does not depend on the type of crime.

Final, the rules on the unusability of evidence shall also apply ex art. 191 c.p.p. under the same conditions as the evidence acquired by search.

***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: It is not possible to change the configuration of the device. Computer Forensics, before proceeding to any operation, shall seal off the mobile device from the network and then proceed with duplication of the data. Any modifications to the device shall be restored (example, changing of passwords). The device must be give back, whether in the case of seizure or search, in the state in which it was found.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter –
www.formobile-

***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: On the basis of L. 18 March 2008, n. 48, ratifying the Council of Europe Convention on Cybercrime drafted in Budapest, 23 Nov. 2001, were introduced some "best practices" regarding acquisition, collection and storage of digital evidences. It is a "best practice" "that behaviour, not necessarily codified, which is considered by the scientific community and technical operators as correct practice to perform certain computer operations on specific devices or media". However, the national regulatory framework does not provide specific rules on use of mobile forensic tools based on artificial intelligence systems.

***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: According to the Italian legal system, where a mobile offence has been committed involving several States, the crime can still be prosecuted in Italy on the basis of artt. 8, 9 and 10 c.p.p., even if partially committed in Italy.

Notably, to ensure that a part of the offence was committed abroad should be a continuing offence; thus, shall be applied art. 8, 3 co. c.p.p. and the jurisdiction lays with the judge ot the country in which the offence was committed, or, if it is an attempted crime, the jurisdiction lays with the judge of the country in which the last act was committed to the commission of the crime.

Otherwise, where it is not possible to determine jurisdiction in such manner, on the basis of art. 9, co. 1, c.p.p., the court of the last place where a part of the action was brought shall have jurisdiction.

In this context, prevailing law stated that these crimes are of relevance to the Italian legal system in their entirety, including the part of conduct that is carried out abroad and, therefore, must be assessed and punished by the Italian judges in their entirety, having regard also to the modalities and gravity of the part of the action occurred in foreign countries (Cass. Pen., VI sez., 17 Feb. 1994).

So, it will be sufficient that the offence committed by means of the mobile device has even partially affected the Italian territory to legitimise the prosecution by the Italian Authority.

Such elements shall be, even if superficially, brought to the attention of the Computer Forensics, that in any case has some basic legal notions and is always supported by the Judicial Police, in turn coordinated by the Public Prosecutor.

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

Answer: Yes, there are. The European Investigation Order (EIO) does not appear to be the only instrument applicable to the cross-border collection of evidence in EU countries. Under certain conditions, European legislation does not preclude the possibility of applying other international conventions of mutual assistance in criminal matters. According to this, art. 34, co. 3, Eu Directive 2014/41 states that: "in addition to this Directive, all Member States may conclude or continue to apply bilateral or multilateral agreements or arrangements with others Member States after the 22 May 2017, only where they enable the objectives of this Directive and contribute to the simplification or further facilitation of procedures of collection of evidences, provided that the level of safeguards laid down in this Directive is respected."

***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?*

formobile@netlaw.bg
Linkedin – Formobile-
Twitter –
www.formobile-

Answer: Please, refer to the RIM's case.

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

Answer: There are no cooperation mechanisms or practices between private entities, except the possibility of appointing technical advisers in case of defensive investigations ex art. 391 bis c.p.p.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter –
www.formobile-

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

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

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

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

Answer: The acquisition of data on mobile devices is not, according to the Italian criminal law, covered by specific safeguards. This is because according to prevailing case law *"The computer data acquired from the phone memory used by the suspect (SMS, whatsapp messages, "downloaded" e-mail messages and/or stored in the memory of the mobile phone) shall be considered as documents on the basis of art. 234 c.p.p. The relative acquired activity does not subject neither to the rules established for the correspondence, nor to the regulation of telephone tapping. In accordance with the teaching of the Supreme Court, it is not possible to apply the discipline dictated by art. 254 c.p.p. with reference to Whatsapp and SMS messages found in a seized mobile phone, as these texts do not be included within the concept of "correspondence", the concept of which involves an ongoing delivery activity, or in any case set in motion by the sender by delivery to third parties for delivery."* (Cass., Sez. V pen., sent. N. 1822/2017). Thus, the activity of acquisition of IT data shall be considered as not subject to any restrictions using the so-called forensic copy, method of acquisition fully compliant with the law, which aims to protect in

formobile@netlaw.bg
Linkedin – Formobile-
Twitter –
www.formobile-

the interests of all parties to the proceedings the integrity and reliability of the data acquired. On the other hand, the Italian Supreme Court, in other judgments, already had occasion to consider that the seizure of mobile devices containing data was entirely lawful, then given back following extraction of the forensic copy, because "*analysis for the selection of accounting documents is particularly complex sweeping the full activity of the suspect. Nor the operations of extracting copies of documents relevant for that purpose could have been carried out on the spot in a limited period of time, sweeping the analysis for the selection a significant activity of study and analysis in order to make a possible selection*" (Cass., Sez. V pen., sent. N. 25527 /2016).

The data thus acquired shall form documentary evidence in criminal proceedings, will be stored throughout the process and after become res judicata, stored in the appropriate registry.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter –
www.formobile-

Section 3: Admissibility of evidence before court

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

Answer: No, there are not.

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

Answer: Data acquired by mobile forensic tools shall be qualified as documentary evidence following the general rules on the acquisition of such types of evidence, as well as the rules of unusability on the basis of art. 191 c.p.p.

Particularly, according to Italian Crime Procedure Law, this type of proof may also be obtained by copying, when the original cannot be obtained and is prohibited, under penalty of unusability ex art. 191 c.p.p., to acquire data containing information on current voices in the public around the facts involved in the process or on the general morality of the parties, witnesses, technical advisers and experts (art. 234, co. 2 and 3, c.p.p.).

With respect to the banning above, it should be made clear that in any case all the data present on mobile devices are acquired and then a selection of those eligible, in accordance with the above provision, and of those who, though produced in judgment, anyway would be unusable ex art. 191 c.p.p. because they would laid into "hearsay".

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?*

formobile@netlaw.bg
Linkedin – Formobile-
Twitter –
www.formobile-

Answer: No, in any case evidence gathered in violation of the provisions of the Criminal Procedure Code, as above, may be used in court. Failure to comply with the rules on evidence always results in unusability ex art. 191 c.p.p.

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

Answer: It doesn't matter that the Cloud is located abroad, whether part of the criminal conduct or one of its events occurred/manifested in Italy the jurisdiction lays with the Italian Courts (as noted above).

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

Answer: The mobile device cannot be altered in any way, not accidentally or willingly. Indeed, this would constitute a clear violation of the provisions on seizure and search of the device as noted above, and would lead to the unusability of the acquired data on the device on the basis of art. 191 c.p.p., regardless of the extent of the alteration.

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.*

formobile@netlaw.bg
Linkedin – Formobile-
Twitter –
www.formobile-

Answer: No, the important thing is that the device is given back to the state in which it was found by Judicial Police and by Computer Forensics.

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

Answer: . See answer 47.

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

Answer: No, they follow the rules of documentary evidence (see answer 39).

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

Answer: See answer 37.

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:

Case 1

formobile@netlaw.bg
Linkedin – Formobile-
Twitter –
www.formobile-

The case relates to the appeal in cassation in which the defendant complains of the defect of unusability of the IT expertise provided by the Computer Forensics on the basis of the acquisition and consequent duplication of computer data present on the defendant's smartphone. Particularly, the Criminal Police had backed up the defendant's whatsapp conversations, which was placed in different whatsapp groups (including also foreign Whatsapp profiles) on which were inserted propaganda messages of ISIS. Furthermore, were acquired videos downloaded and stored in the internal memory of the mobile phone concerning Jihad, the exaltation of martyrdom and the repression of Western infidels. The defendant's attorney objected the unusability of those elements ex art. 191 c.p.p., because the guarantees provided for the accomplishment non-repeatable technical assessment had not been respected, consisting of the presence of the defender, and the possibility of appointing a party technical adviser. However, in the Court's view, the complaint raised by the defence cannot be accepted, as established case law "*the extraction of data held in a computer device, if performed by experienced personnel able to avoid the loss of the same data, represents repeatable technical verification[…] as a purely mechanical operation reproducible for an indefinite number of times*" (Cass., sez. V pen., sent. N. 22066/2020).

Case 2

The Italian Supreme Court upheld the defendant's action alleging the incorrect legal classification carried out by the Court of Appeal concerning the nature of the verification carried out for the finding of data resulted for data extraction on a mobile device. Particularly, the Court of Appeal declared the technical expertise unusable because based on the acquisition of IT data without the guarantees due to one-time assessment on the basis of L. n. 48/2008. In this case, the Supreme Court noted that *"the legislation referred to in the Law n. 48/2008 is limited to imposing the retention and non-alteration of data, but does not prescribe the adoption of predetermined*

formobile@netlaw.bg
Linkedin – Formobile-
Twitter –
www.formobile-

modalities; such acts cannot therefore be classified as unrepeatable; in the present case we acknowledge that none of the data in the computer device has been modified; the Court of Appeal confused access to computer data with alteration; Law n. 48/2008 does not impose specific procedures but arrangements to obtain a reliable result of evidence." (Cass., sez. II pen., sent. N. 29061/2015).

Case 3

The defendant proposed grounds for appeal to the Supreme Court considering the provisions violated on the basis of artt. 247, co. 1-bis and 260, co. 2, c.p.p., because the technical measures were not observed to ensure the preservation of originals or to prevent alteration of the seized computer equipment. Specifically, the Public Prosecutor's IT consultant would not have indicated the "hash" value of files obtained from computer devices, ,which in the defendant's opinion is always necessary to ensure that the copy is in conformity with the original, and its immodificability. However, the Supreme Court has established that the assumptions of the defendant's defence were not founded, noting that *"Art. 247 c.p.p., co. 1 bis, provides that, in the event of a search of a computer or telematic system, technical measures are to be taken to ensure the retention of original data in order to avoid any alteration. Art. 260, co. 2, provides that copy of data, information or computer programs subject to seizure it must be carried out on suitable supports, by a procedure ensuring that the copy is in conformity with the original and its immodificability. None of these provisions, however, suggests that, in the case of extraction of copies of computer data, it is necessary to indicate the "hash" value of these data in order to validate their authenticity, not having the legislator typed technical measures and procedures to ensure the retention of original data to prevent alteration. Nor, moreover, has the defence even proposed, in substance, the lack of correspondence between the extracted copies and the data originally present on computer devices in the availability of the defendant."* (Cass., sez. III Pen., 28 May 2015).

formobile@netlaw.bg
Linkedin – Formobile-
Twitter –
www.formobile-

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

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

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

Answer: All evidence acquired in crime process are assessed in accordance with the principle of free conviction of the judge, whereby there is no tied evaluation of certain evidences, but are freely assessed by the judge in the manner deemed most appropriate. The only limitation to this discretionary power is the duty to state reasons on the basis of art. 192, co. 1, that provides "the Judge assess the evidence by giving account in the justification of the results obtained and the criteria adopted".

So, this general principle also applies to the assessment of IT data acquired in crime process. Regarding the professional requirements of the forensic computer consultants, at the moment the law does not provide any typical requirement, not requiring registration in professional registers. Consequently, the Public Prosecutor or the Judge notionally may appoint any person. The only limit is to be identified in art. 221 c.p.p., which provides that the consultant has "special skills in the specific discipline".

formobile@netlaw.bg
Linkedin – Formobile-
Twitter –
www.formobile-

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: No, see the previous answer.

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: No, see answer 48.

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: The basic rule of evidence collection is provided by art. 191 c.p.p. "Evidence acquired in violation of the prohibitions established by law shall not be used"; a confirmation of the substantial importance of the data, which therefore is not reduced to mere formal frills, the Italian legislator has predicted that "*The unusability is also detectable automatically in every state of the procedure*".

Additionally, Sent. Cost. n. 219/2019, the Italian Constitutional Court stated as inadmissible the questions of constitutional legitimacy with reference to art. 2, 3, 13, 14, 24, 97 c. 2 and 117 co. 1 (related to art. 8 European Convention on Human Rights) Cost., art. 191 c.p.p., in so far as it, according to the prevailing interpretation in the case law of legality, does not foresee that the

unusability also concerns the evidential outcomes, including seizure of the body of the crime or of the items pertaining to the crime, the acts of search and inspection carried out by the Judicial police excepting all cases envisaged by law or otherwise not validated by the judicial authority by a reasoned decision.

The Constitutional Legitimacy review was concerning the widely debated issue of the relationship between search and seizure: the current case law denies that the illegality of the search is propagated to the following seizure, having almost unanimously accepted the conclusions (contradictory to the premise that the judgment affirms the argument of derived invalidity except that the body of the crime and the things pertaining to the crime may always be susceptible to seizure: and as in the criminal trial all real evidence belongs to the crime, all relevant evidence, however discovered, is available» (F. Cordero, Procedura penale, Milano, 2012, p. 649) of the Supreme Court, that in 1996 stated that «*if it is true that the illegality of the search for evidence of the criminal offence, when it assumes the dimensions resulting from a clear violation the rules for the protection of subjective rights subject to specific protection by the Constitution, cannot, in general, not spread its disabling effects are the results that research has allowed to acquire, it is also true that when that research, however carried out, ended with the discovery and seizure of the body of the crime or things pertaining to the crime, it is the procedural system itself which considers entirely irrelevant the manner in which that seizure was reached*» (Cass., Sez. Un., 27 March 1996).

The Constitutional Court, in its judgment in question, stated that, in the absence of an express legislative provision, is «*the same regulatory system to endorse the conclusion that the unusability resulting from the breach of an evidentiary prohibition, a principle of 'derived unusability' cannot be applied*».

Then summarizing, the Criminal Procedure Code state the arrangements for collecting and submitting evidence during the trial with rules that apply to any type of evidence.

formobile@netlaw.bg
Linkedin – Formobile-
Twitter –
www.formobile-

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: No, any evidence extracted via mobile forensics tools shall be classified as just evidence, always and in any case shall apply the rules dictated by the code in the matter of collecting evidence; equality between the prosecution and defence is guaranteed by the possibility for the parties to carry out defense investigations, on the basis of artt. 391 bis and ss c.p.p.

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: There is no training requirement for any of the parties to the proceedings. For Computer Forensics, see the answer n. 48.

54. **Question:** *Is there a predetermined 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: There are no special rules on data acquired from mobile devices. The procedure and duration shall be determined by the court in the case of appointment of the IT expert (on the basis of art. 224, co. 1, c.p.p.) or by the Public Prosecutor /defendant's defence or civil party, in the case of party technical consultancy. The results of the activity carried out by the Technical Expert are

collected in the expert report submitted to the judge within a specified period granted by the expert at his request (art. 227 c.p.p.)

***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:

Suspect/Defendant (they are supplied with the same guarantees on the basis of art. 61)

The guarantees and procedural rights of the defendant are provided ex artt. 64 e 65 c.p.p. whereby "The suspect, even if in custody or in custody for another reason, is able to intervene free in the interrogation, without prejudice to the precautions necessary to prevent the flight risk, or violence. They shall not be used, even with the consent of the person questioned, methods or techniques likely to affect the freedom of self-determination or to alter the ability to remember and assess facts. Before the interrogation starts, the person shall be advised that:

a)his statements can always be used against him;

b) except to the extent that art. 66, co. 1, provides otherwise, has the power not to answer any questions, but the process will follow its course;

c) whether it will make statements of facts concerning the responsibility of others, will assume, with regard to these facts, the role of witness, except incompatibilities provided by art. 197 and the guarantees whereby art. 197-bis. Failure to comply with the provisions referred to in co. 3, let. a) and b) shall be unusable the statements made by the person interrogated. In the absence of the warning referred to in co. 3, let. c), any statements made by the person interrogated on facts which relate to the liability of others are not usable against them and the person interrogated shall not be able, in respect of those facts, to take on the role of witness (art. 64 c.p.p.).

formobile@netlaw.bg
Linkedin – Formobile-
Twitter –
www.formobile-

On the basis of art. 65 c.p.p. the suspect has the right to know from the Public Prosecutor *"in a clear and precise form the fact attributed to him; the Public Prosecutor makes known the evidence against; and if it cannot be prejudicial to investigations, tells him the sources. Invites, therefore, the person to explain what he considers useful for his defense and and directly asks the questions. If the person refuses to answer, it shall be recorded in the minutes. The minutes shall also mention, where appropriate, the physical features and any particular signs of the person."*

Final, on the basis of art. 96 c.p.p. the defendant has the right to appoint one or more legal counsel, otherwise a public defender will be appointed on the basis of art. 97 c.p.p.

Injured party

On the basis of art. 90 c.p.p. the injured party may, in each state and grade of the process, submit pleadings and provide evidence. This right, where the injured person has died as a result of the offence, is up to his/her close relatives.

The injured person may constitute himself in the criminal trial as a civil party on the basis of art. 78 c.p.p., by means of a lawyer for the purpose appointed ex artt. 96 c.p.p., for being recognize the damage where it is established that the offence was committed by the hands of the defendant.

Public prosecutor

The Public Prosecutor prosecutes on the basis of art. 50, where there are no grounds for motion to dismiss.

Leads the investigation, thus authorizes the Criminal Investigation to perform certain investigative acts or validates its performance in the case of urgent acts (specifically, as above).

May submits written submissions, requires the admission of evidence, including deposition.

The Judge

Even to the Judge is granted a supplementary power of initiative on the basis of art. 507, c.p.p., where the taking of certain evidence is absolutely necessary.

In any case, on the basis of art. 506 c.p.p. he can intervene during the examination of witnesses or private parties.

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: the answer is given in the previous paragraphs, in particular with reference to the Blackberry case.

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: On this point, too, the previous answers apply, in particular with reference to the art. 191 c.p.p.

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: The principle of the free conviction of the judge always applies in criminal proceedings, which is balanced by the judge's obligation to state reasons. On the basis of art. 192 c.p.p., indeed, "*the judge evaluates the evidence taking into account in the motivation of the acquired results and*

the criteria". In the Italian legal system there is the maxim "*Iudex peritus peritorum*", that means "*The judge shall be the expert among experts*". Indeed, the Judge is not bound by the result of the expert report and may depart from or completely disregard the conclusions reached by the expert. In such case must give an adequate justification for its choice (Cass., sez. IV, 13 Dec. 2010). The judge may also agree to the conclusions reached by a party consultant or may appoint a new expert(cfr. Cass., sez. I, 8 May 2003).

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: During the investigation phase all evidence is covered by a secret investigation and therefore are not accessible to the parties unless a request for review is made (in case of application of protective measures).

Indeed, art. 329 c.p.p. provides that "*Acts of investigation carried out by the public prosecutor and the judicial police, the requests of the public prosecutor for authorization to carry out investigative acts and the acts of the court providing for such requests sare kept secret until the accused has knowledge of them, and, however, no later than the closing of preliminary investigations*". Also, art. 116 c.p.p. "*During the proceedings, any person interested therein may obtain copies, extracts or certificates of individual acts*" adding that "*The request shall be decided by the public prosecutor or the judge who proceeds at the time of the application, or after the procedure has been determined, the President of the College, or the judge who issued the dismissal order or sentence".*

formobile@netlaw.bg
Linkedin – Formobile-
Twitter –
www.formobile-

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: The Italian Criminal Procedure Code, art. 198, provides that "*the witness has the obligation to present himself to the judge and to comply with the prescriptions given by the same for the procedural requirements and to answer the questions according to truth"* and moreover "*the witness cannot be obliged to give evidence on facts from which his criminal responsibility may arise*".

Art. 199, also provides that "*The defendant's next of kin are not obligated to testify. They must however give evidence when they have filed a complaint, complaint or request or they or a next of kin are offended by the crime*"; to demonstrate the importance of this provision the code, in paragraph 2 of the provision "*the judge, under penalty of nullity, informs the aforementioned persons of the right to abstain asking them whether they intend to use it*".

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: Victims are protected during the investigation by the confidentiality of the investigation, in addition to protective measures which can be applied in the case of specific crimes. As for the privacy of those involved in the investigation, with perhaps media relevance, the Code provides

for a prohibition on the publication of investigative acts which are still kept secret.The main problem, however, is in relation to the press and mass media more generally than, on several occasions, especially in the case of investigations with strong media coverage, that cloaking behind the "right to report" violates that prohibition.

Art. 684 c.p. punish by arrest or fine *anyone who publishes, in whole or in part, including by summary or by way of information, documents or documents relating to criminal proceedings,whose publication is prohibited by law.*

The scope of the precept can only be understood by reference to the Criminal Procedure Code specifically prohibiting the publication of procedural acts, on the basis of, particularly, artt. 114 and 329 c.p.p.

The first provision prohibits publication, whether in part or in summary form, by means of the press or other means of distribution, acts covered by secrecy or even just their content (paragraph 1); also prohibits the publication, even partial, of acts no longer covered by secrecy until the preliminary investigation is completed, or until the end of the preliminary hearing (paragraph 2); if the hearing is held, publication shall not be permitted, even partial, of the documents in the public prosecutor's file, if not after delivery of the judgment in appeal grade (paragraph 3); while it sets as a general rule that the content of acts not covered by secrecy may always be published (paragraph 7).

The second rule, on the other hand, enshrines the secrecy of investigative acts, until the defendant becomes aware of it, and by the way no later than the closing of preliminary investigations (first paragraph); when necessary for the continuation of investigation sthe public prosecutor may permit the publication of individual acts or parts thereof (second paragraph). Even when acts are no longer covered by secrecy, the public prosecutor, if necessary for the continuation of investigations, may by reasoned decree provide for the obligation of secrecy for individual acts or the prohibition to publish the content of individual acts or news relating to certain operations (third paragraph).

The United Sections of the Supreme Court, in the judgment in comment, highlight how in our legal system there is no complete coincidence between the security grading and the disclosure grading

and that therefore there is *a double filter at the publication of acts*: *an absolute prohibition of publication, even partial or by summary… of acts covered by the confidentiality of investigations or even their content, ex art. 329 c.p.p., funtil the defendant is unaware of it and, in any event, not later than the closure of the preliminary investigation; is a ban, limited to textual elements only, in force, with the remodelling carried out by the Constitutional Court, beyond such a time barrier, until the end of the preliminary hearing (paragraph 2) and, if a hearing is held, until the decision in appeal grade (paragraph 3).*

That means that art. 684 c.p. is different according to the stage of the procedure to which the covered act belongs; if during the preliminary investigation phase this ratio is to be identified the need not to compromise the evidence acquisition phase, subsequently, and specifically during the trial the aim of the legislator is to safeguard the serenity of the judge, which must be as free from external conditioning as possible, so as to allow the full operation of the principle of adversarial between the parties placed in a position of (trend) parity.

Having said this, it is therefore necessary to determine whether, in addition to the public interest in the good performance of the process, (variously declined depending on the stage of the procedure, as briefly examined above) the interest of the parties involved in ensuring that news is not disseminated may also be identified, related to the same procedure, which concern them and therefore whether the intended case punishable by art. 684 c.p. whether or not it is multi-offensive.

In the civil case law the pluri-offensive nature of the offence in question has often been stated, as the rule has been read as intended to protect, alongside the public interest, also dignity and the reputation of those involved in the trial.

The criminal case law, equally long established positions open to recognition of the pluri-offensive nature of the offence, has recently recalled a strand dating back to the ‘80 decade, recognising the reasons for the ban on the basis of art. 624 c.p. and art. 114 c.p.p., not only and not so much in the protection of the suspect, but in safeguarding the fundamental principles of the accusatory process; consequently, this seems to require an indirect guarantee, and therefore of mere fact of the interests of the parties involved in the process, not being their confidentiality the legal asset directly targeted by the norm.

Having taken note of this contrast, the Supreme Court referred the matter to the United Sections, which have decided to adhere to the guideline which excludes the pluri-offensive nature of the offence ex 684 c.p., thereby denying the right of the private party to compensation for the damage arising from the violation of that rule.

According to the Court, the cornerstone of such an exegetical landing is last paragraph of art. 114 c.p.p., that provides that "the content of acts not covered by secrecy may always be published". Indeed, the legislator has granted to the right to inform and speculate right to be informed (Cost. Court n. 112/1993; n. 153/1987; art. 10, par 2 CEDU; Cass. civ. 10 Oct. 2014, n. 21404; Cass. civ. 4 Sep. 2012, n. 14822) the maximum that could reasonably allow the need to safeguard even the principles of the accusatory trial, avoiding that the chosen model, aimed at ensuring the training of the trial, in the contradictory of accusation and defense, become the empty simulacrum of a rite that he had recovered in other ways the formulas deemed suitable to create prejudices in the mind of the judge.

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: There are not more elements, in Italian legal system, concerning the use of mobile forensics in criminal investigations that we should report, in addition to what has already been said.