Preparatory Colloquium
24 – 27 September 2013, Antalya (Turkey)
Section III: Information Society and Penal Law

NATIONAL REPORT – ITALY*

Giulio ILLUMINATI*

B) General Questions

1) Are there current (legal or socio-legal) definitions for applications of IT and ICT within the context of criminal procedure (including forensics)? How such conceptual definitions reflected in the literature, legislation, court decisions, and relevant practices within the context of the criminal process?

Italy ratified the Council of Europe Convention on Cybercrime in 2008. Accordingly, it has amended and strengthened its Criminal and Procedural Codes to include comprehensive coverage of computer crimes and cybercrime and to introduce specific rules governing investigative measures in the IT and ICT domains. The aim of the Budapest Convention was to adapt traditional investigative measure to the new cyber world using technological devices. Specific needs of the cyber criminal phenomena asked for new instruments provided by the Budapest Convention such as the collection of evidence in electronic form, the interception of content data and traffic data, the expedite preservation of content and traffic data, the production orders of digital data.

Nevertheless, the Italian system still shows a lack of specific definitions on several pivotal issues.

*The Italian Code of Criminal Procedure (CCP) gives only few definitions concerning the IT and ICT applications currently provided in relation to investigative measures. Article 266-*bis *CCP regulates the interception of digital or technological communications as the investigative measure to be used against crimes committed via an information technology system or other computing or Internet communication systems. It allows the real-time collection and recording of content data of specified communications transmitted by means of a computer or other technological digital systems or a group of interconnected or related devices. To this aim, the law defines the object of the interception as the "flow of communications pertaining to computerized or electronic systems, or otherwise among several systems". The conditions and guarantees of such interception are the same as those provided for wiretapping of telephone conversations or other forms of communication (see D.1.b below).*

(2) Are there specific institutions and/or task forces involved in the implementation of ICT within the criminal justice system?

Italian law enforcement agencies involved in criminal investigation are usually the State police and the Arma dei Carabinieri*. Within the police there is a specialised unit called "*Polizia postale*"; it carries out investigations involving correspondence and in particular IT and ICT communications but this is not an exclusive competence.*

(3) Are there private (commercial) organisations (companies) that offer ICT related services to the criminal justice system? If so, can you give examples? What limits have to be observed?

Every commercial company involved in the ICT market has the duty to cooperate offering their services to the criminal justice enforcement agencies. Specific protocols have been ratified between law enforcement agencies and ICT service providers but their contents are not public.

(C) Information and Intelligence: building information positions1 for law enforcement

(1) Which ICT-related techniques are used for building information positions for law enforcement agencies?

Digital intelligence (Digint) is a powerful tool used by law enforcement agencies in order to prevent and to combat serious crimes. To achieve its aims intelligence services use every ICT-related techniques at his disposal. No specific regulation lists what measures might be adopted by intelligence services. The sole provisions concerning specifically intelligence secret surveillance are related to preventive interceptions (see C.4 below) and special covert investigation to tackle child abuse on the Internet targeting paedophile predators online. The special measure is provided by Article 14 of Law n. 269 of 1998 according to which policemen may open phishing websites, enter chat rooms, adopt controlled purchases of pictures or delay arrest or seizures. Ex ante *judicial authorization is required and the results may be used in trial.*

---

* Important notice: this text is the last original version of the national report sent by the author. The Review has not assured any editorial revision of it.

* University of Bologna.

(2) To which type of public (e.g. DNA databases) and private (e.g. PNR or financial data such as SWIFT data) databases do law enforcement agencies have access?

Italian law enforcement agencies have access to several public and private databases. Law enforcement agencies may have access to every database when it is provided for by law. In principle no limitation is given to the access by law enforcement agencies for public purposes to private databases. Hindrances may be justified in order to protect professional privileges (e.g. attorney-client privilege, physician-patient privilege, journalists' privilege).

*Italy has recently implemented the Treaty of Prüm, introducing DNA profiling and DNA database (see Law n. 85 of 2009, and Articles 133, 224-*bis*, 359-*bis*, 392 CCP). The person who is asked to give a DNA sample may refuse. In that case the compulsory taking of the sample is allowed only when the investigation is referred to crimes punished by life imprisonment or a maximum imprisonment higher than three years(see Article 224-*bis *CCP) and it must be done by an expert under authorisation of the judge of the preliminary investigation. An emergency procedure is described by Article 359-*bis *CCP: when the delay can be prejudicial to the investigation, the Public Prosecutor can coerce an immediate execution. But he/she needs a subsequent validation, within 48 hours, from the judge.*

Unfortunately protocols related to the present time management of DNA database haven't so far been adopted. As a consequence, law enforcement agencies are using and storing DNA profiles for criminal justice purposes without a significant and appropriate legal framework. However, the Corte di cassazione *has ruled that informal data banks built up by police forces on their own initiative are lawful.*

(3) Can techniques labelled as data mining and data matching be applied? If so, can these techniques be used to create profiles of potential perpetrators or risk groups? If so, have special tools been developed for law enforcement agencies?

Italian law does not provide for specific rules governing data mining or data matching, except for DNA data mining, as mentioned above, question C(2). Nevertheless these techniques are commonly used by law enforcement agencies in order to create profiles of potential criminals especially in the framework of intelligence investigations or crime prevention. Unfortunately these measures have no legal basis and often they are not even reported in investigation records.

(4) Can coercive measures (e.g. interception of telecommunications) be used for building up information positions?

*According to Article 226 of the implementation rules (*disposizioni di attuazione*) to the CCP*, *the Minister of Home affairs or the secret services supervisors as his proxies, the police commissioner (*Questore*) or financial police commissioner may request the public prosecutor to be authorised to intercept traditional or digital telecommunications or to put domestic premises under acoustic surveillance when it is necessary for discovering facts related to serious crimes such as organised crime or drug trafficking. In this case the investigative measure is not directed to gathering evidence to be used in a criminal trial. Its aim is to provide useful information in order to prevent crime.*

The public prosecutor shall authorise the interception when there are sufficient grounds to support the need for preventive procedure. The order has to state specific reasons that justify the measure. Authorisation lasts for no more than 40 days; prorogation for further 20 days may be granted. Operations are concisely recorded and the public prosecutor has the duty to destroy the records immediately after the end of the operations.

The same proceedings apply to the interception of telephone or digital traffic data or to any other relevant data concerning traditional or digital telecommunications available to service providers.

According to Law n. 144 of 2005, the said preventive interceptions have been permitted also in order to fight terrorism or crimes of subversion of the Constitutional order or mafia crimes. The request can be made by the Prime minister or by the directors of intelligence agencies acting as his proxies, and has to be authorized by the General Prosecutor to the Court of appeal of the place where the target is located. The authorisation is issued by an order providing reasons for the absolute need of the measure. Time limits are established in 40 days; prorogation is allowed upon reasoned authorization of the general prosecutor of the Court of appeal.

The above mentioned provisions are deemed to be consistent with the Constitutional principles protecting the privacy of communications. Since 1973 the Constitutional Court has recognised the lawfulness of secret surveillance measures even when they merely intend to prevent serious crimes.

Some scholars consider both ordinary and anti-terrorism preventive interceptions as a breach of the Constitutional provisions stating the need for a judicial authorisation for any measure impinging on fundamental rights because the authorization is left to the Public prosecutor office.

No use in criminal trial can be made of the data collected by preventive interceptions. Law enforcement agencies cannot open an investigation starting from the results of the preventive interception and no report can enter the investigation file.

(5) Which private actors (e.g. internet providers or telecom companies) retain or are obliged to retain information for law enforcement agencies?

Pursuant to Article 132 para. 1 of the Privacy Code (Legislative Decree n. 196 of 2003), any private actors acting as an IC service provider offering its services on communications public networks is compelled to retain information for law enforcement agencies. The data must be retained for no longer than 12 or 24 months (see D.2 below) and then be erased.

(6) Which private actors can provide or are obliged to provide information to law enforcement agencies?

Pursuant to Article 132 para. 2 of the Privacy Code, private actors acting as a service provider are obliged to provide information to law enforcement agencies upon request of

- the public prosecutor office, even requested by the victim;

- the defence of the suspect.

(7) Is there judicial control on building information positions?

*In general terms, individuals aware of mistreatments of their private information may apply for review to an independent body named "*Autorità Garante per la protezione dei dati personali*". This authority does not qualify as judicial authority.*

Information on traffic data to law enforcement authorities requires a preventive request from the public prosecutor. No specific judicial review is provided for intelligence. If the information is designed for being part of the materials of a criminal case, ordinary judicial controls apply consequently.

(D) ICT in the criminal investigation

(1) Can law enforcement agencies carry out interception in real time of a) e-traffic data; b) content data?

a) *Real time collection of e-traffic data is allowed by Italian law for criminal justice purposes as an exception to the general obligation to erase personal data. This measure is regulated by Article 132 para. 4-*ter *and 4-*quater *of the Privacy Code, as lastly modified by Legislative Decree n. 109 of 2008 to comply with the Directive 2006/24/EC that imposed a shorter time limit on the duty for the system providers to store traffic data. The law adopts a large definition of personal data: it covers the IP address, telephone or mobile numbers, e-mails and any other digital data useful to identify the source, the destination, the time or the duration of a call or of a digital communication.*

Providers are obliged to store traffic data for 24 months and digital data for 12 months starting from the date of the telecommunication. Data related to no answer calls data must be retained for no more than 30 days.

In order to obtain e-traffic data for investigative purposes an order of the public prosecutor is required. The defence or the victim may apply for such order to the public prosecutor. The defence may also request system providers directly to obtain e-traffic data but in this case the application must specify that the lack of those data might jeopardise the investigation of the defence.

b) *Real time collection of content data concerning IT communications is provided for by Article 266-*bis *CCP which defines the interception of digital or technological communications as the investigative measure to be used against any crime committed via an information technology system or other computing or Internet communication system. It allows real-time collection and recording of content data of specified communications transmitted by means of a computer or other technological digital systems or a group of interconnected or related devices. The procedure to be followed is the same provided for by law for telephone wiretappings (Articles 266-271 CCP): requirements are a strong suspicion that a crime has been committed; the seriousness of the crime; the absolute need of the interception to go on on with investigations. Interceptions are admissible even for investigation against unknown persons. The prosecutor must apply for an authorization to the judge of the preliminary investigation who decides in writing delivering a warrant. In exigent cases, the prosecutor may start to intercept but he needs a judicial validation within 48 hours. Every person can be the target of an interception but privileges concerning professional secrets and State secret apply. Operations must be carried out by the prosecutor but he can authorize the police to use their own devices. The interception can last 15 days and may be extended for further periods of 15 days as long as the judge is satisfied that the requirements are still fulfilled.*

All the interceptions must be fully recorded and they need to be transcript by an expert before being admitted into the materials of the case. An in camera hearing is provided in order to select the relevant materials. An exclusionary rule applies when rules governing the requirements or the operational issues are not followed. As a consequence, those data cannot be used in trial and must be destroyed (Article 271 CCP). Any interested person can request the judge that all records of the interception be destroyed when they are not necessary for the proceedings

Special provisions concerning the Prime Minister and the members of the Government and of Parliament require a political authorization before the interception may start (see Article 68 of the Italian Constitution and Article 10 of the Constitutional Law n. 1 of 1989). The Constitutional Court recently ruled that the President of the Republic cannot be the target of a surveillance measure and whenever his statements are accidently recorded, they must be immediately destroyed without preventive discovery.

(2) Can law enforcement agencies have access to/freeze/search/seize information systems for a) e-traffic data; b) content data?

In order to fulfil the international obligations provided by the Budapest Convention on cybercrime, Italy has updated its criminal procedure rules introducing new investigative measures or extending the previous rules to the IC and ICT related techniques. In other words, Law n. 48 of 2008 has extended the objects of traditional investigative techniques to the digital world.

Results are not fully satisfactory. Some scholars underline the fact that Italy has lost the opportunity to introduce a complete and coherent legal framework. In other words, it has failed to achieve the implementation of digital forensics best practices in order to collect, preserve, and present electronic evidence in ways that best ensure and reflect their integrity and irrefutable authenticity. A clearer legal framework on the use of scientifically derived and proven methods toward the preservation, collection, validation,

identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources would have been appropriate.

Search and seizure

Law n. 48 of 2008 has modified several rules with the aim to comprise digital data within the possible objects of the investigative measures.

Article 244 CCP provides for a legal framework related to digital inspections. The public prosecutor may order an inspection of IC and ICT devices in order to obtain criminal traces, images or data. Every operation must grant the integrity and the genuineness of the computer original data.

*According to Article 247 para. 1-*bis *CCP, the public prosecutor orders the search of a computer system or part of it and computer data stored therein, even those encrypted or protected by other means when he has reasons to believe that there are data, software or information relevant for the criminal investigation. Operations have to be carried out with the aim to maintain both the authenticity and the integrity of the computer data. Digital search concerns any digital data (including both traffic and content data).*

In order to have a full overview of the rules governing searches and seizures, it is appropriate to consider other provisions governing the powers of the police in exigent cases. Pursuant to Article 354 CCP, as amended by Law n. 48 of 2008, the police have the duty to preserve the integrity of the digital data, adopting any technical measure they deem to be useful to avoid any modification. Police must provide, if possible, to copy digital data granting the conformity to the original data.

As a general rule, searches can be carried out during pre-trial investigation in force of a warrant of the public prosecutor. Searches of premises or body search may be carried autonomously by the police in exigent cases, i.e. when a person is caught in the act of committing a crime (Article 352 CCP). In those cases validation by the public prosecutor must intervene within 48 hours. In those cases the police may intervene adopting any measure they deem necessary in order to preserve digital data from modification. Police may search a computer system or part of it and computer data stored therein, even those encrypted or protected by other means when they have reasons to believe that there are data, software or information relevant for the criminal investigation and there is a risk they can be deleted.

Seizure usually concerns the computer data (including both traffic and content data) but it does not concern the hardware. The latter is usually returned to the owner after the computer memory has been cloned. As a consequence, the Corte di cassazione *has ruled that the defendant may not apply for a judicial review of the seizure as such (created through a clone) because of the lack of a relevant interest. Scholars criticized that decision because the Court didn't seem to consider the dangerous implication bound to the cloning.*

*Article 254-*bis *CCP deals with the seizure of digital data stored by private companies acting as service providers. The judicial authority may seize those data or a copy adopting a proceeding granting the authenticity and the integrity of the data.*

Seizure of digital data does not represent an infringement of fundamental rights of the individual granted by Article 8 ECHR and by Articles 2 and 15 of the Italian Constitution. To this aim, no indiscriminate access and recording of personal information stored in a personal computer is admissible. According to the Corte di cassazione*, the seizure warrant must precisely state which is the crime to be investigated and what is the link with the seized data.*

The seized computer data must be committed in custody to the registrar. According to Article 259 para. 2 CCP, the custodian must preserve the integrity of the digital data preventing any unauthorized access. To this aim, the seized digital data must be protected by specific seals ordered by the judicial authority (Article 260 CCP). Seals may have a digital nature. A copy of any relevant data can be obtained using technological devices and procedures (such as the hash functions), granting the conformity of the copy to the original data and its continuity.

Digital and ICT communications may be seized in force of an order of the public prosecutor. In exigent cases, the police may ask the public prosecutor to be authorized to freeze the contents as provided by Article 353 CCP. In those cases the police may delay or suspend the forwarding.

Production orders

Pursuant to Article 248 CCP, a search can be avoided if the relevant data are delivered directly by the owner. To this aim, law enforcement agencies may have access to the computer or the digital network in order to pinpoint the relevant data.

A production order is provided by Article 256 CCP according to which professionals and public servants protected by specific privileges must promptly provide the judicial authority (i.e. the public prosecutor) with all the data, information or software at their disposal; the delivery of a certified copy is allowed. Cautions are prescribed for cases in which the delivery of the data could infringe a professional privilege. A special procedure concerning State secret applies. This measure postulates a duty to cooperate with law enforcement agencies.

(3) Can telecom companies or service providers be obliged to share data with law enforcement agencies? In case of noncompliance, are there any coercive measures or sanctions?

Yes. See answers to questions D.1 and D.2 on production orders. Non compliance might even result in a criminal offence.

(4) May law enforcement agencies apply video surveillance? Can they oblige natural or legal persons to cooperate?

Italian current criminal procedure does not provide any specific rule governing video surveillance. Nevertheless this measure is applied during the pre-trial stage and the legal basis varies according to the nature of the surveillance.

In order to define the applicable law, a threefold approach is necessary:

1. *Audio or video recording made by private persons is considered as a document and it may enter the criminal proceedings according to the rules governing the admissibility of documents. Documents are broadly defined by law as instruments representing facts, persons or things (Article 234 CCP).*

Therefore audiovisual documents are usually admissible as evidence in trial unless they fall within the scope of some specific exclusionary rule. In this light, video surveillance as an investigative measure is carried out by law enforcement agencies and it is subject to the general rules on preliminary investigation provided for by the Code.

2. *As regards the place where the surveillance takes place, it is necessary to distinguish between, public space. private sphere and "places implying an expectation of privacy" (an intermediate category created by the case law embracing those places that are different from domestic premises but in which private behaviours take place, such as public toilets or club privés).*

Images gathered in force of video surveillance in a public space are not covered by constitutional provisions granting privacy to the individuals. As a consequence, video surveillance in public spaces is an investigative measure usually carried out by the police and it does not require any preventive judicial authorisation. It can be used as evidence in trial.

Likewise, video surveillance carried out for private purposes such as CCTV can be used in trial and natural or legal persons must cooperate with law enforcement agencies acting for criminal investigation purposes. They follow the rules governing documentary evidence.

In the so-called places implying expectation of privacy an authorisation of the public prosecutor is needed in order to carry out a video surveillance. When such surveillance implies the tapping of conversations, rules governing interceptions apply accordingly and in particular a warrant issued by the judge is required (see before, D.1.b).

3. *When private premises are involved a difference arise depending on the object of the visual surveillance, i.e. whether it concerns communicative or not communicative behaviours.*

*Video or acoustic surveillance in private premises concerning communicative behaviour is subject to the same rules governing telephone tapping. The legal definition is meaningful: Italian law defines this kind of interference as "*intercettazione di comunicazioni tra presenti*". In order to intercept communications between present persons in domestic premises, Article 266 para. 2 CCP requires, as an additional condition, the concrete suspicion that criminal behaviour is still ongoing inside.*

Video surveillance in private premises related to non communicative behaviour (mere behaviour) is forbidden in force of a decision of the Corte di cassazione*, confirmed by the Constitutional Court: the lack of a specific regulation concerning the requirements, thresholds and limits of video surveillance measure does not fulfil the Constitutional provisions governing the right to inviolability of private homes (Article 14).*

(5) May or must law enforcement agencies apply audio-visual recording of interrogations (suspects, witnesses)?

*Article 141-*bis *CCP sets out the rules governing the recording of the questioning of the suspect. In particular, when the interrogation of the suspect under arrest or of the suspect held in custody intervenes outside a hearing, it must be fully audio or video recorded. An exclusionary rule affects the unrecorded statements of the suspect. In case specialised police or technical devices are lacking, the recording has to be carried out by an expert. Transcription is provided only upon request of the prosecutor or of the defence.*

(E) ICT and evidence

(The chain of stages: collecting/storing/retaining/producing/presenting/evaluating electronic evidence)

(1) Are there any rules on evidence that are specific for ICT-related information?

No.

(2) Are there any rules on integrity (e.g. tampering with or improper processing) and security (e.g. hacking) of ICT-related evidence?

*Even updating specific measures related to digital investigation, the Italian law did not provide for specific rules granting both the integrity and the security of ICT-related evidence. Several provisions concern the need to preserve the integrity or improper processing of digital data or other ICT-evidence. They are mostly related to inspection, search and seizure (see above, D.2). According to Article 244 CCP, concerning the digital inspections, the court may order any control or any technical overview also related to ICT or digital systems, or adopt any technical measures in order to grant the digital data integrity and to prevent any manipulation. A similar rule is provided by Article 247 para. 1-*bis *CCP.*

As mentioned above, the law does not explicitly specify which are the proper proceedings, storing cautions or technical measures to be adopted during the operations in order to preserve the digital evidence. The law merely specifies the duty for the law enforcement agency to grant integrity and security of ICT related evidence without saying how to pursue this aim. It seems clear that best practices must be adopted in gathering and storing any digital data. One might consider that best practices are often unpredictable by law because of the rapidity of the technological development.

(3) Are there any rules on admissibility (incl. the principle of procedural legality) of evidence that are specific for ICT-related information?

No specific rule governs the admissibility of ICT-related information. Ordinary rules apply: evidence is admissible if it is relevant and it is not prohibited in force of an exclusionary rule concerning its lawfulness.

(4) Are there any specific rules on discovery and disclosure for ICT-related evidence?

Specific rules are given for the interceptions of IT and ICT content data. They follow the procedure provided for interceptions of telephone communication according to which at the end of the operations the defence has the right to have access to the records in order to select the relevant data and to obtain a prompt exclusion of the irrelevant ones. This filter proceeding is conducted in front of the judge (see above, D.1).

(5) Are there any special rules for evaluating (probative value) ICT-related evidence?

No specific rule is given.

(F) ICT in the trial stage

(1) How can or must ICT related evidence be introduced in the trial?

No specific rule is given for ICT-related evidence.

When the applicable rules are those concerning interceptions, they apply accordingly. In particular, the admissibility of the selected records in trial implies that their transcription has to be made by an expert. The transcript records are admissible as evidence in trial and no further formality is required.

(2) Can distant interrogations (e.g. by satellite connections) be applied?

*Distant interrogation of the defendant follows the rules provided for regulating his participation in trial via video connection. According to Article 146-*bis *of the implementation rules to the CCP, videoconferences are allowed to grant the participation of the defendant, following a reasoned judicial order, when these three conditions are fulfilled:*

- *the case concerns a serious crime (as listed by Article 51 para. 3-*bis *and Article 407 para. 2, lett.* a*, n. 4 CCP),*
- *the defendant is held in custody and there are serious reasons of public order or public security*
- *the trial is complex and there is a reasonable risk that ensuring the defendant's physical presence would delay the trial phase.*

*A further autonomous case concerns the defendant serving a term of imprisonment pursuant to Article 41-*bis *of the Prison Law implying a special restrictive regime.*

*Distant interrogation of a witness is applicable as well. According to Article 147-*bis *of the implementation rules to the CCP, the court, even on its own motion, may order a videoconference when:*

- *the trial concerns some serious organised crimes and the person to be examined is put through special protective measures. The distant interrogation in this case tends to avoid the high risk for the person to be examined to be physically present in trial;*
- *the person to be examined has changed his/her personal details as a consequence if his/her role in the criminal investigation. In this case special cautions apply, such as the ban to film his/her face;*
- *the defendant is accused of one of the crimes listed in Article 51 para. 3-*bis *and in Article 407 para.2 lett.* a*, n. 4 CCP and he has to be examined as a co-defendant in a joint trial;*
- *the interrogation concerns undercover agents and they have to be examined on the activities carried out during the undercover operations. Even in this case the face of the person has not to be shown.*

Precondition for a distant interrogation in trial is the fact that there is no absolute need for the presence of the person to be examined in court.

(3) Can digital and virtual techniques be used for the reconstruction of events (killings, traffic accidents)?

*Italian law does not provide for any specific rule governing the virtual reconstruction of events. The legal reference for this investigative technique may be found in rules governing the so-called "*esperimento giudiziale*", a judicial reconstruction of the crime. To this aim, specialised units of digital forensic police and specific software are used, such as RiTriDEC (*Ricostruzione Tridimensionale della Dinamica dell'Evento Criminale*, tridimensional reconstruction of the criminal event) and S.A.S.C. (*Sistema di Analisi della Scena del Crimine*, crime scene analysis system).*

(4) Can audio-visual techniques be used to present evidence at trial (in its simplest form: pictures and sound)?

Yes but no specific rule is provided. The prosecutor or all the other parties, with leave of the court, can use audio or visual techniques as a support to present their arguments before the court, but such materials are not evidence themselves, unless they have been admitted as documentary evidence (in the sense explained above, D.4.1).

Expert witness may also use digital techniques in order to explain their reports before the court. Those materials are part of the expert final report.

(5) Can criminal "paper" case files be replaced by "electronic ones"? Are there any developments towards digitalising of the trial proceedings?

Case files containing several documents are often scanned and the defence or the victim may ask for a digital copy of the materials of the case. Nevertheless, digital copy did not replace the "paper file" that is still the sole document with a legal value in trial.