Section 4: Concept paper and questionnaire *
Italian system*

(B) Jurisdictional issues

(1)(a) How does your country locate the place of the commission of a crime in cyberspace?

No specific provision regulates the issue concerning the identification of the *locus commissidelicti* in case of cybercrimes.

Cybercrimes are therefore subject to the general rules on jurisdiction laid down by the Criminal Code ("CodicePenale", hereafter c.p.).

Following the ***principle of territoriality***, jurisdiction is exercised by Italian Courts over nationals and foreign citizens, when the offence is committed within the Italian territory (an offence is considered to have been committed in Italy (1) when the action or the omission is committed, in whole or in part, within the Italian territory or (2) when the harm occurs within the Italian territory (*principle of ubiquity)*, art. 6.2 c.p.).

In case of offences committed abroad, Italian Courts can immediately proceed against Italian and foreign citizens:

a) for particular crimes offending the interests of the State, as expressly indicated by art. 7, ns 1), 2), 3) c.p. (according to the ***principle of defense or of passive personality*)**;

b) for offences committed by Public officials in the service of the State in case of abuse of power or violation of duties relating to their functions (***principle of nationality or of active personality*)**, art. 7 n. 4) c.p.;

c) for all the offences for which laws or international treaties entitle Italian Courts to proceed (***principle of universality*** (i.e. Italian Courts have jurisdiction regardless the nationality of the offender, the victim and the place where the offence was committed), art. 7 n. 5)c.p.

Further provisions under General part of the Criminal code deal with political offences committed abroad by nationals or foreign citizens (art. 8 c.p.), common offences committed abroad by a national (art. 9 c. p.) or by a foreign citizen (art. 10 c.p.), (in these cases, the exercise of jurisdiction is subject to different procedural or/and substantial requirements).

Save for offences under art. 7 n. 1)c.p., political offences (art. 8.3c.p.) committed abroad by a national or a foreign person are punished under Italian law on a request of the Minister of Justice (art. 8.1 c.p.)and, with respect to specific offences, upon complaint of the offended person (art. 8.2 c.p.).

Following the *principle of nationality*, the national who commits abroad a common offence punishable under Italian law by life imprisonment or by deprivation of liberty for no less than three years is punished under Italian law, if he/she is present within the Italian territory (art. 9.1

*Subsections B and C are by MariavaleriadelTufo. Subsections D, E, and F are by TommasoRafaraci.

* 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.

c.p.). In case the offence is punishable by deprivation of liberty for a shorter period, a request by the Justice Minister, or a petition or a complaint submitted by the offended person is also required (art. 9.2c.p.).

If the offences were committed against a foreign State, the European Union or a foreign citizen, the national offender is punished on request of the Justice Minister, unless extradition has not been granted (art. 9.3c.p.).

Following the *principle of defense*, the foreign person who commits abroad a common offence against the Italian State or against a national, which is punished under Italian law by life imprisonment or by deprivation of liberty for no less than one years is punished under Italian law, if he/she is present within the Italian territory, on request of the Justice Minister, or on petition or complaint of the offended person (art. 10.1c.p.).

Following the *principle of universality*, if the offence was committed abroad by a foreign person against a foreign State, the European Union or a foreign citizen, the offender is punished under Italian law if (1) he/she is present within the Italian territory; (2) the offence is punishable by life imprisonment or by deprivation of liberty for no less than three years; (3) the extradition has not been granted to the State where the offence was committed or to the State to which the foreign offender belongs (art. 10.2 c.p.).

The special part of the Criminal code establishes special jurisdictional rules in particular cases: the law 3.VIII.1998 n. 269, introducing in the Criminal code sexual offences against children, provides Italian jurisdiction over such crimes as well as over other sexual crimes, when the offence is committed abroad by a national, or against a national, or by a foreign citizen in complicity with a national, in this last case provided that the minimum penalty is five years and the Justice Minister so requests (art. 604 c.p.).

As far as cybercrimes are concerned, Italy (L. 18.III.2008 n. 48) has ratified and implemented the European Convention of Budapest on Cybercrime, 23.XI.2001. Jurisdictional issues, regulated by art. 22 of the Convention, were not specifically implemented. Nevertheless, the Italian system complies with the Convention requirements, as well as with the jurisdictional requirements under art. 10 of the Framework Decision 2005/222/JHA on attacks against information systems.

Prima facie, problems could arise with respect to art. 22.1.d) of the Budapest Convention. The European instrument obliges the States to claim jurisdiction over offences committed *by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.* This provision could lead to a lack of jurisdiction under art. 9 c.p. establishing jurisdiction over offences committed by a national outside the Italian territory, because, as explained above, art. 9 c.p. recognizes Italian jurisdiction over offences committed by a national abroad only to a certain extent.

Nevertheless, a result consistent with art. 22.1.d) of the Budapest Convention could be obtained applying art. 7.5 c.p., automatically recognizing no conditioned domestic jurisdiction over a crime, as long as an international treaty so provides.

(b) Does your national law consider it necessary and possible to locate the place where information and evidence is held? Where is the information that one can find on the web? Is it where the computer of the user is physically present? Is it there where the provider of the network has its (legal or factual) seat? Which provider? Or is it the place where the individual who made the data available? If these questions are not considered to be legally relevant, please state why.

Under criminal proceedings, it is necessary to locate the place where information and evidence is held. This place depends on the type of information or evidence sought. The information found on the web can be considered as evidence collected in Italy, but other information concerning who made it available and how may be necessary. From this perspective location of evidence depends on where is the provider or the individual who made the data available. As far as provisional measures are concerned, if the provider or the individual is in Italy, general rules apply. If the provider or the individual is abroad, there are no specific rules and the Prosecutor may use the general instruments of international cooperation.

(2) Can cybercrime do without a determination of the locus delicti in your criminal justice system? Why (not)?

The determination of the place where the offence was committed is necessary for claiming jurisdiction, because the applicable rules change depending on where the offence was committed (in Italy or abroad).

In general Italian jurisdiction can be easily claimed under the territorial principle, since the *locus delicti*is identified under the principle of ubiquity (Italian Courts exercise jurisdiction even if just a segment of the fact occurred within the borders, therefore the territory principle is applied with respect of a very large number of offences, included cybercrimes). Nevertheless, when the offence cannot be considered as committed within the territory of the State, jurisdiction can also be claimed, but conditions and requirements as provided by law (arts 9 and 10 c.p.) shall be satisfied. For instance, problems can arise if the offence committed abroad is punished under Italian law with a period of imprisonment which does not reach the minimum penalty to claim jurisdiction under arts 9 and 10 c.p. There is no limit to Italian jurisdiction when an international treaty recognizes Italian jurisdiction over the offence (art. 7 n. 5c.p.). In this case the *locus delicti*has no relevance and jurisdiction is claimed without any condition).

Under a procedural point of view, it shall be stressed that the investigations can begin regardless of the *locus delicti*, but the Prosecutor shall in any case indicate where the offence took place when he/she charges the defendant asking for the indictment (art. 417 of the Code of Criminal Procedure, "Codice di procedurapenale", hereafterc.p.p.). The decree of indictment issued by the

Judge for preliminary hearing shall indicate the *locus delicti* , otherwise it is null and void (art. 429 c.p.p.).

(3) Which jurisdictional rules apply to cybercrime like hate speech via internet, hacking, attacks on computer systems etc.? If your state does not have jurisdiction over such offences, is that considered to be problematic?

Conducts such as hate speech via internet, hacking, attacks on computer systems etc. are established under domestic criminal law as offences punishable with severe penalties, therefore, also when the offence is committed abroad and the other jurisdictional requirements are satisfied, jurisdiction can be claimed.

(4) Does your national law provide rules on the prevention or settlement of conflicts of jurisdiction? Is there any practice on it?

The prevention and the settlement of conflicts of jurisdiction is a relevant and urgent issue, particularly because the increasing transnational crime can easily lead to an overlapping of jurisdictions, which should be avoided. The principle of *ne bis in idem* is expressly recognized in Italian law only in relation to domestic proceedings. As far as international jurisdictional conflicts are concerned, the system provides very basic rules under arts 9 and 10 of the Criminal Code (1930): jurisdiction is not claimed over offences committed abroad if extradition has been accorded. Nevertheless, also if a foreign final decision on the same matter has been already issued, art.11 c.p. claims Italian jurisdiction over offences committed in Italy by a national or a foreign offender. Italian jurisdiction is claimed as well as over offences under artt. 7,8,9,10 c.p. committed abroad by a national or a foreign offender, provided that Justice Minister so requests. On the contrary the Code of Criminal Procedure (1988) does not allow to extradite or to proceed for the same facts (art. 739) when a foreign decision was recognized for execution purposes by national law (art. 731).

The problem of pending proceedings at international level is taken in account also by the d.ls. 231/2001 establishing the administrative liability of legal entities arising from a crime. As an exception to the general rule, there is no liability for legal entities having their seat in Italy in case the State of *commissidelicti*s proceeding for the fact.

Regardless of the national provisions, it should be stressed that Italy is bound by the Conventions it has ratified and by the instruments of the European Union. Furthermore, as far as international relationships are concerned, international general principles and treaties have priority on domestic law. Although the principle of *ne bis in idem* at international level is not yet generally recognized as *jus cogens*, the implemented policy by the Council of Europe (see first the European Convention of Extradition of 1957) and by the European Union (from Schengen to Lisbon, with the strong

support of the Court of Justice) aims at the enforcement of the principle of *ne bis in idem* among States and the mutual recognition of judicial decisions. That is why the Italian system is complying with European standards.
As far as the prevention of conflicts of jurisdiction is concerned, the European Convention of extradition of 1957 and other treaties on specific offences regulate the situation of pending proceedings. With respect to cybercrime, Italy is bound, at European level, by the Framework Decision 2009/948/JHA, not yet implemented, but having effects within the limits of such an act. The Framework Decision aims to prevent situations where the same person is subject to parallel criminal proceedings in different Member States and to avoid the final infringement of the principle of *ne bis in idem* by direct consultations among Member States who have jurisdiction, in order to reach consensus on an effective solution. Likewise the Budapest Convention expressly establishes under art. 22.5 an obligation to mutual consult, where appropriate, when more than one State has jurisdiction over the same offence. Within the Italian legislation, the question of compatibility between renunciation of criminal proceedings and jurisdictional principles at constitutional level is considered to be surmountable: therefore the obligations laid down by the two European instruments should be considered as having direct effects into the domestic system.

(5) Can cybercrime do without jurisdictional principles in your criminal justice system, which would in essence mean that national criminal law is applicable universally? Should this be limited to certain crimes, or be conditional on the basis of a treaty?
The principle of universality applies in the Italian system under art. 7 n. 5) c.p. without limits or conditions, provided that an international treaty obliges the State to exercise domestic jurisdiction over specific crimes under such a principle. The provision of art. 7 n. 5) operates automatically, i.e. the domestic law does not need to enact specific jurisdictional rules to comply with the obligation under the convention. Any type of crime can be subject to the universality principle.

(C) Substantive criminal law and sanctions

1) Which cybercrime offences under your national criminal justice system do you consider to have a transnational dimension?
Following the law 16.III.2006 n. 146 ratifying and implementing the Palermo Convention on transnational organized crime, the conventional definition of transnational offence (art. 3) was introduced into Italian criminal system. Therefore an offence is considered transnational if punished at least with four years of imprisonment and (a) it is committed in more than one State or (b) it is committed in one State, but a substantial part of its preparation, planning, direction or

control takes place in another State; or (c) it is committed in one State, but involves an organized criminal group that engages in criminal activities in more than one State; or (d) it is committed in one State, but has substantial effects in another State.
As far as cybercrimes are concerned, the relevance of this technical definition shall be checked on a case by case basis. In more general terms, transnationality is in most cases a distinctive feature of cybercrimes. In fact many relevant cyber offences in this matter were introduced in the criminal code just by ratifying and implementing the Budapest Convention (l. 18.III.2008, n. 48), which aims to set up a "*common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation*".

2) To what extent do definitions of cybercrime offences contain jurisdictional elements?
No jurisdictional elements are contained in the definitions of cybercrimes.

3) To what extent do general part rules on commission, conspiracy or any other form of participation contain jurisdictional elements?
According to Italian general rules, a crime (and of course a cybercrime) is considered as having been committed in Italy also when only a part of the conduct of one of the participants in the offence occurred in Italy. In this case, also the other participants in the offence acting abroad are considered punishable under Italian criminal law. For instance the act of aiding and abetting in Italy is sufficient for Italian Courts to exercise jurisdiction over a cybercrime which took place entirely abroad, according to the principle of territoriality (the crime is just considered as having been committed within the Italian territory).

4) Do you consider cybercrime offences a matter that a state can regulate on its own? If so, please state how a state may do that. If not, please state why it cannot do that.
Cybercrime is not a matter that a State can regulate on its own because of the "a-territoriality", which constitutes in many cases one of its main features. Italy has began to criminalize cyber offences in 1993, in the absence of international obligations in this sense. Further interventions were made according to the Budapest Convention and the Framework Decision 2005/222/JHA on attacks against information system. By the development of technology, crimes harmonization and effective cooperation are the only weapons to fight transnational offences such as cybercrimes, which cannot be controlled by a single State for their nature and characteristics.

5) Does your national criminal provide for criminal responsibility for (international) corporations/providers?

The Italian system provides for administrative liability for legal entities arising from specific crimes, under particular conditions (D.ls 8.VI.2001 n. 231). Offences which may give raise to such liability shall be specified by the law. The law 18.III.2008 n. 48 introduced in the D.ls. 2001/231 a provision (art. 24 *bis*) including cybercrimes among such offences.
Cybercrimes, included in the criminal code, in respect of which the liability of legal entities is extended are the following:

- illegal access to a computer or telematics system (art. 615 *ter* c.p.);
- illegal interception, obstruction or interruption of computer or telematics communications (art. 617 *quater*);
- installation of equipment for intercepting, preventing or interrupting computer or telematics communications (art. 617 *quinquies*),
- Damaging computer information, data and programs (635 *bis*);
- Damaging computer information, data and programs used by the State or by another public or public utility entity (635 *ter*);
- Damaging computer or telematics systems (635 *quater*);
- Damaging computer or telematics system of public utility (635 *quinquies*)

6) Does the attribution of responsibility have any jurisdictional implications?

As far as jurisdiction is concerned, art. 4 of D.ls. 2001/231 states the liability of legal entities having their principal seat in Italy also with respect to offences committed abroad, according to artt. 7, 8, 9, 10 c.p., provided that the State of *commissidelicti* is not proceeding for the same fact. In case of legal entities having their principal seat abroad, the scholarship and the jurisprudence recognize Italian jurisdiction in case of offences committed in Italy.

D) Judicial cooperation in criminal matters

1) To what extent do specificities of information technology change the nature of mutual assistance?

First. Information technology can facilitate mutual legal assistance without changing its nature, thanks to new forms of communication and transmission as far as requests, answers and, in general, communications between authorities are concerned.
Second. Specificities of information technology make it possible to carry out traditional activities, such as testimony, without the need for people to move to a foreign State (e.g. videoconference, skype). However, it is difficult to believe that these new methods could be applied without the assistance of the authority of the State (or States) involved. This assistance might be different

from traditional assistance and might be limitedto assure the fairness and correctness of the evidence.

This scenario is far from allowing "a virtual courtroom, in which hearings may take place, whilst nobody is present in the real courtroom". Sensitive questions, which the technique of videoconference already raises,concern the respect of the guarantees of fair trial (e.g. the right to confrontation). Allowing a trial via videolinkin order to establish a higher threshold for prosecutorial extradition,seems to beunlikely in the international context. The need to guarantee the respect of the presumption of innocence and the right to liberty of the defendant (also in relation to provisional measures) would require a very high level of trust between States.

Third. Traditional mutual legal assistance may be bypassedto the extent in which data and information can be obtained directly from public databases, or from other sources (when the consent is given), or spontaneously from the person who owns information and that information refers to. But,if data and information obtained without any formal requirement are to be used as evidence at trial, concerns on admissibility may arise. In particular, hearsay rules may represent an obstacle.

2)(a) Does your country provide for the interception of (wireless) telecommunication? Under which conditions?

The Italian Code of Criminal Procedure allows interception of wireless telecommunication under the same conditions applicable for any other kind of interception of communication (there is not an *ad hoc* provision). These conditions are: a) the offence of the proceedings must be one falling under the provided list (very serious crimes); b) there is strong evidence that a crime of those listed has been actually committed; and c) interception is indispensable for the prosecution of investigations (Artt. 266 and 267 c.p.p.).

These conditions also apply to interception of IT communications, as expressly provided for by Art. 266-*bis*c.p.p., where specific reference is made to cybercrimes, i.e. computer crimes or common offences committed by the use of ICT (in addition to the listed crimes mentioned above).

The interception must be authorised by the judge upon a request of the public prosecutor. In case of urgency, the public prosecutor alone can order the interception; however, this order has to be followed by a decision of the judge.

An atypical case of interception of telecommunication and IT communication is provided for by Art. 226 disp. att. c.p.p., according to which interception is allowed for the prevention of very serious crimes, relating mainly to organized crime and terrorism. In this case, it is the Ministry of Interior to ask the public prosecutor for an authorisation, issued when there are elements that show the need of crime prevention and that interception is deemed necessary for this purpose.

2)(b) To what extent is relevant that a provider or satellite may be located outside the borders of the country?

In the absence of a specific legislation on this matter, according to the case law of the Italian Court of Cassation, what is relevant is the nationality of the service provider ("nazionalitàdell'utenzatelefonica"). Italian authorities are allowed to intercept an Italian cell phone, regardless the cell phone is used outside Italy. In this case, there is no need for the Italian authorities to send a request of legal assistance to the State where the cell phone is used. According to the Court of Cassation, the cell phone is subjected to the legislation of the State of the provider.

Similarly, the Court of Cassation has affirmed that Italian authorities are allowed to intercept communications from a foreign phone if the phone of the recipient is Italian and is being intercepted. In this case too, there is no need for the Italian authorities to send a request of legal assistance (this is the so-called "istradamento" theory).

2(c) Does your national law provide for mutual legal assistance concerning interception of telecommunication? Did your country conclude international conventions on it?

Italian law does not provide for mutual legal assistance specifically concerning interception of telecommunications. However, a request of legal assistance concerning this kind of investigative measure is considered to fall under the scope of application of mutual legal assistance as provided under the Italian Code of Criminal Procedure.

Italy has signed and ratified the 1959 Council of Europe Convention on mutual legal assistance, which does not expressly provide for interception of telecommunication. However, according to the principle of *favor rogatoriae* under art. 1 of the said Convention, the Italian Court of Cassation has affirmed that interception of telecommunications falls within the scope of the said Convention.

Italy has signed the 2000 EU Convention on mutual legal assistance, where some provisions are entirely devoted to mutual legal assistance for the purpose of interception of telecommunications. However, Italy has failed to ratify it,therefore this instrument is not yet enforceable.

Italy has not signed the II Protocol to the 1959 Council of Europe Convention on mutual legal assistance, where provisions on mutual legal assistance for the purpose of interception of telecommunications (very similar to those provided for under the 2000 EU Convention) are foreseen.

Italy has signed and ratified the 2001 Council of Europe Convention on Cybercrime, where specific provisions concern: (i) mutual assistance for real-time collection of traffic data associated with specified communications transmitted by means of a computer system; and (ii) mutual

assistance for real-time collection or recording of content data of specified communications transmitted by means of a computer system.

3) To what extent do general grounds for refusal apply concerning internet searches and other means to look into computers and networks located elsewhere?

Under the Italian Code of Criminal Procedure (Artt. 723 and 724) general grounds for refusal have a twofold nature.

Some grounds for refusal can be opposed by the Ministry of Justice if: (i) the request is likely to prejudice the sovereignty, security, or other essential interests of the State; (ii) execution of the letters rogatory is contrary to national law or fundamental principles; (iii) there are grounded reason to suspect that the request has been issued for the purpose of prosecuting a person on account of his or her sex, racial or ethnic origin, religion, nationality, language, political opinions, or personal or social conditions, in case the defendant has not given the consent to the execution of the rogatory; (iv) the requesting authority does not provide guarantees in favor of the person that is to be heard; (v) reciprocity does not apply with the requesting State.

If internet searches or other investigation measures requested by a foreign authority are liable to affect one of these interests or guarantees, the Ministry of Justice can stop the execution of a rogatory.

Other grounds for refusal can be opposed by the judicial authority, after the rogatory has passed the examination by the Ministry of Justice, if: (i) the execution of the letters rogatory is contrary to national law or legal principles; (ii) the offence motivating the letters rogatory is not punishable under Italian law (the requirement of double criminality is not satisfied); (iii) there are grounded reason to suspect that the request has been issued for the purpose of prosecuting a person on account of his or her sex, racial or ethnic origin, religion, nationality, language, political opinions, or personal or social conditions, in case the defendant has not given the consent to the execution of the rogatory.

In the absence of any specific provision, these general grounds for refusal may well apply to internet searches *etsimilia* to the same extent in which they apply to any other kind of measure requested by rogatory.

4) Is in your national law the double criminality requirement for cooperation justified in situations in which the perpetrator caused effects from a State in which the conduct was allowed into a State where the conduct is criminalised?

The relevant factor for the satisfaction of the requirement of double criminality is that either a conduct or its harmful effects is criminal under Italian law. If not, refusal of legal assistance on the ground of double criminality is legitimate.

5) Does your national law allow for extraterritorial investigations? Under which conditions?

Extraterritorial investigations can be carried out only by means of mutual legal assistance. Italian authorities cannot carry out investigations autonomously outside their national territory because of lack of competence/jurisdiction. They can delegate this activity to the competent authorities of the State where investigations are to be carried out, through a request of legal assistance.

The 2000 EU Convention and the EU Framework Decision 2002/465/JHA, which both provide for the setting up of Joint Investigation Teams for the purpose of carrying out transnational investigations, have not been ratified or implemented by Italy.

The Italian Code of Criminal Procedure does not either permit extraterritorial investigations carried out by the defence. According to the Italian Court of Cassation, defence lawyers are not legitimated to carry out this kind of activity abroad. They can only ask the competent authority to send a rogatory (this is the so called "canalizzazione" theory, according to which any activity must be canalised via the public authority).

6) Is *self-service* permitted? What conditions should be fulfilled in order to allow *self-service*? What is the practice in your country?

Under Italian law, in principle,self-serviceshould not be permitted. According to the Italian Code of Criminal Procedure, a request of legal assistance is always necessary.

A case that may be assimilated to self-service and is permitted according to the case law of the Court of Cassation concerns interception of wireless communication where Italian cell phones are used abroad or foreign phones get into contact with Italian phones (see answer nr. 2-b).

Another case of self-service may be constituted by direct consultation of DNA databases by national authorities, as provided for within the European Union. However, only very basic information can be obtained via self-service. If extra information on a DNA profile is needed, a request of legal assistance should be put forward.

7) If so, does this legislation also apply to searches to be performed on the publicly accessible web or in computers located outside the country?

The case law and the legislation concerning these specific cases of self-service should not apply outside their limited scope of application (interception of wireless communications and consultation of DNA data).

8) Is your country a party to Passenger Name Record (PNR), financial transactions, DNA exchange, visa matters or similar agreements? Please specify and state how the exchange of data is implemented into national law.

Does your country have an on call unit that is staffed on a 24/7 basis to exchange data?

Italy takes part to:

- S.I.S. andS.I.R.E.N.E.
- the Visa Information System (V.I.S.)
- the automated Customs Information System (C.I.S.)
- the European Dactylographic System (Eurodac)

In all these cases, information and data are exchanged via central databases.

Italy allow for the exchange of:

- DNA and dactyloscopic data
- information on criminal records in the framework of the "Network of Judicial Registers" pilot project (together with other 10 EU Member States: Belgium, the Czech Republic, France, Germany, Spain, Luxembourg, the Netherlands, Poland, Slovakia and the UK)
- information extracted from the criminal record between Member States, via the European Criminal Records Information System (Ecris)
- data and information for the purpose of investigating child pornography and similar offences against children, via the C.E.T.S. (Child Exploitation Tracking System).

In all these cases, data are exchanged either by direct access to national databases or upon request.

Italy is also party to the EC Directive 2006/24 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks, and amending the EC Directive 2002/58, which obligates the providers of publicly available electronic communications services or of public communications networks to ensure that data is available for the purpose of the investigation, detection and prosecution of serious crimes.

Under the Italian legislation, most of the time, the authority deemed competent for the exchange of information and data are both judicial authorities and police officials (either by own initiative or after delegation by the public prosecutor).

By a Declaration contained in a letter from the Permanent Representative of Italy, dated 19 June 2009, registered at the Secretariat General on 22 June 2009 and updated by a letter from the Permanent Representative of Italy, dated 9 June 2010, registered at the Secretariat General on 9 June 2010, in accordance with Article 35, para. 1, of the Council of Europe Convention on Cybercrime of 2001, Italy has designatedthe "ServizioPoliziaPostale e delleComuniczioni" of the Ministry of Interior as point of contact for the network 24/7:

Servizio Polizia Postale e delle Comunicazioni

Via Tuscolana 1548, Roma
Email: htcemergency@interno.it

9) To what extent will data referred to in your answer to the previous question be exchanged for criminal investigation and on which legal basis? To what extent does the person involved have the possibility to prevent/correct/delete information? To what extent can this information be used as evidence? Does the law of your country allow for a Notice and Take-Down of a website containing illegal information? Is there a practice? Does the seat of the provider, owner of the site or any other foreign element play a role?

In the absence of any specific legislation, data referred to in the previous answer can be exchanged for criminal investigation and crime prevention.

According to the Italian Court of Cassation, spontaneous exchange of information between police authorities (without a formal request)is lawful, even in the absence of a specific agreement.

As far as the Schengen Information System is concerned, art. 11 of Law n. 388 of 30 September 1993 (which ratified the Convention implementing the Schengen Agreement) provides that access to, correction and deletion of information can be requested by the interested person to the national Data Protection Supervisor who decides on the basis of a feedback by the Ministry of Justice (the central authority competent for the S.I.S.) or after direct verification and control.

The right to access by the interested person can be limited when it could hinder the pursuing of the objective for which information has been filed in the system, or when it is necessary to safeguard other persons' interests, or when information is highlighted for discrete surveillance.

As far as DNA data are concerned, according to Law n. 85 of 30 June 2009 (which implementedthe EU Decision 2008/615/JHA), national authorities have to cancel DNA data and destroy the biological sample if the person involved in criminal proceedings is found not guilty, or after a corpse has been identified, or if a missing person is located.

Cancellation of DNA data and destruction of the biological sample are also foreseen when the genetic profile has been obtained in violation of law.

In any case, data shallnot be retained after 40 years since the occurrence of the circumstance that justified the filing of the data, and samples shall not be retained after 20 years since the occurrence of the circumstance that justified the collection of the sample.The national Data Protection Supervisor exercises controlling power over the DNA database.

Where there are no specific provisions, the "Code on the protection of personal data" (Decretolegislativo n. 196 of 30 June 2003) applies.According to Art. 7, the interested person enjoys the right to ask: the update, rectification or integration of data; the cancellation of data; its transformation into anonymous data; the locking of data treated in violation of law. However,

according to Art. 8, these rights cannot be exercised when data are used for justice purposes or when the purpose of criminal investigations may be hindered.

Information and dataexchanged during investigations maybe used as evidence at the trial. They may enter the proceedings as documentary evidence.

According to Art.321 c.p.p., which foresees seizure aimed at the prevention of further offences, during the investigation stage and the trial, access to a website can be denied to Italian usersby an order issued to the service provider.
According to Artt. 254 and 254-*bis*c.p.p., seizure of data/information may be ordered to the service provider also for evidence purposes. In this case the judicial authority may decide that a copy of data/information is made (in the respect of the "chain of custody", so as to guarantee the reliability of the copied data) and may order the service provider to retain and look after the original data/information (without any interruption in the supply of the service).
Seizure for evidence purposes is also possible in relation to electronic mails. Art. 353 para.3c.p.p.provides that electronic correspondence may be seized by an order to the service provider not to forward the mail to its recipient. The order is normally issued by the public prosecutor. In case of urgency, the order may be issued by the police; however, it needs to be followed by the order of the public prosecutor. It must be underlined that this measure is unlikely to be applied, given the high-speed transmission of this kind of mail which makes it almost impossible to stop the mail before it is transmitted to its recipient.
By final decision, confiscation may be ordered.
In any case, the service provider has the obligation to promptly act in order to disable access to a website in Italy, where a notice or an order by the judicial or administrative authority is issued (see Artt. 14, 15 and 16 of "Decretolegislativo" 70/2003, implementing the EC Directive 31/2000 on electronic commerce).
One of the leading cases is the seizure of the foreign *Pirate Bay* website by the order to an Italian service provider to disable access to it in Italy.

The nationality of a website is not relevant. If the judicial authority decides to proceed to the seizure of a website, it issues an order to the Italian service provider, which must disable access to the seized website in Italy.

10) Do you think an international enforcement system to implement decisions in the area of cybercrime is possible? Why (not)?

An international enforcement system to implement decisions in the area of cybercrime may be possible in relation to some very serious crimes which affect national or international security, and more in general interests of an entire community.
In relation to minor cybercrimes there may be some obstacles to such a system, double criminality being the most striking one. What if a criminal conduct in one State constitutes the exercise of a legitimate right in another State? The balance between conflicting interests can be done only at national level and cannot be imposed over a foreign State and its authorities.

11) Does your country allow for direct consultation of national or international databases containing information relevant for criminal investigations (without a request)?
Italy allows direct consultation of DNA and dactyloscopic databases and vehicle registers, according to the EU Framework Decision 2008/615/JHA on the stepping up of cross-border cooperation, implemented by Law n. 85 of 30 June 2009.
Italy also allows for direct consultation of S.I.S. and S.I.R.E.N.E., as provided for under the Convention on the Application of the Schengen Agreement, implemented by Law n. 388 of 30 September 1993.
Italy is party to the TECS-The Europol Computer System and to the Case Management System of Eurojust, wheredirect access and consultation by national members and liaison officers is allowed.
Italy has directaccess to data and information shared at international level via C.E.T.S. (Child Exploitation Tracking System).

12) Does your State participate in Interpol/Europol/Eurojust or any other supranational office dealing with the exchange of information?Under which conditions?
Italy participates in Interpol, Europol and Eurojust.
No specific conditions apply.
However, as far as the exchange of information is concerned, specific provisions under the national implementing measures are as follows:
A) Europol:
According to Art. 5 of Law n. 93 of 23 March 1998 implementing the EU Convention on Europol (now replaced by Decision 2009/371/JHA), the director, deputy directors and duly empowered Europol staff, the members of the management board and other bodies of Europol, the liaison officers, and the police officers working with Europol are under a duty of confidentiality. If they violate thisduty and reveal secret information or aid the revelation of secret information, they may be punished by custodial sentence.
B) Eurojust:

According to Art. 7 of Law n. 41 of 14 March 2005, implementing Decision 2002/187/JHA on Eurojust, the national member can:
(i) request and exchange written information on criminal investigations and criminal proceedings with the competent judicial authority, notwithstanding the dutyof confidentiality upon the public prosecutor and the police concerning ongoing investigations (Art. 329 of the Italian Code of Criminal Procedure);
(ii) request the accessto information on criminal records;
(iii) requestinformation and data filed in the Schengen Information System to the competent national central authority.

E) Human rights concerns

Which human rights or constitutional norms are applicable in the context of criminal investigations using information technology?

In the context of criminal investigations using information technology, the applicable constitutional norms may be:
- Art. 2 on the respect of human dignity
- Art. 3 on the right to equality
- Art. 13 on the right to liberty
- Art. 14 on the right to respect private homes
-Art. 15 on the right to privacy concerning correspondence and any other form of communication
- Art. 24 para. 2 on the right of defence
- Art. 27 on the presumption of innocence
- Art. 111 on the right to a fair trial.

At international level, someprovisions under the European Convention on Human Rights may be of relevance:
- Art. 3 on the prohibition of torture
- Art. 5 on the right to liberty and security
- Art. 6 on the right to a fair trial and the presumption of innocence
- Art. 8 on the right to respect for private and family life.

Also someprovisions of the EU Charter of Fundamental Rights may apply:
- Art. 1 on the inviolability of human dignity
- Art. 7 on the respect for private and family life, home and communications
- Art. 8 on the protection of personal data
- Art. 42 on the right of access to documents
- Art. 47 on the right to a fair trial

- Art. 48 on the presumption of innocence.

Is it for the determination of the applicable human rights rules relevant where the investigations are considered to have been conducted?

No. Under the obligations undertaken by Italy at international level, human rights rules always apply, regardless where investigations have been carried out.

How is the responsibility or accountability of your State involved in international cooperation regulated? Is your State for instance accountable for the use of information collected by another state in violation of international human rights standards?

Italy can be responsible for the use of information collected by another State in violation of international human rights standards to the extent provided for by the ECHR. Italy may be condemned to pay an amount of money for just satisfaction. Once the trial has been found not to be fair, Italy may also be under the obligation to re-open the proceedings.

F) Future developments

Modern telecommunication creates the possibility of contacting accused, victims and witnesses directly over the border. Should this be allowed, and if so, under which conditions? If not, should the classical rules on mutual assistance be applied (request and answer) and why?

A distinction should be drawn between the stage of criminal investigation and the trial.

During investigation, direct contacts with the victims or potential witnesses (not also with the suspect) may be allowed, even by informal contacts and without the involvement of the competent authorities of the State where these persons are.

During the trial, for evidence purposes (or during the investigation for the purpose of obtaining information to be admitted directly in court), contacting accused, victims and witnesses directly over the border, without a formal request, may not be easily allowed. Classical rules on mutual legal assistance may apply. The assistance of the authority of the requested State is necessary for two main reasons:

i) to guarantee the lawfulness of the evidence, which in part is formed in the requested State, where the person to be heard is;

ii)to guarantee the rights of the person to be heard, who may have the right to be assisted by a lawyer, or enjoy immunity or other privileges under the law of both the requesting and the requested State.

See also under D), answer to question n. 1.

Is there any legal impediment under the law of your country to court hearings via the screen (skype or other means) in transnational cases? If so which? If not, is there any practice?

Under the Italian Code of Criminal Procedure hearings by videoconference, both at national and international level, are expressly provided for (see Artt. 146-*bis*, 147-*bis* and 205-*ter*disp. att.c.p.p.). In fact, Italy has a quite long-standing tradition in hearings by videoconference, mostly carried out in cases concerning organized crime, where it is not appropriate for security reasons to move a detainee from a place to another for the purpose of taking testimony.

The necessary condition for carrying out hearings by videoconference in transnational cases is that an agreement must be concluded between Italy and the foreign State involved.

A legal impediment concerns the hearing by videoconference of the defendant in transnational cases: only if he or she is in custody abroad, hearing by videoconference can be carried out.