Preparatory Colloquium
Verona (Italy), *28 – 30 November 2012*
Section I - Information Society and Penal Law

ITALY

Carlenrico PALIERO*

Section 1

(A) Scope of questionnaire (see Annex 1 and Annex 2)

The questions in this Section generally deal with "cyber crime." This term is understood to cover criminal conduct that affectsinterests associated with the use of information and communication technology (ICT), such as the proper functioning of computersystems and the internet, the privacy and integrity of data stored or transferred in or through ICT, or the virtual identity of internet

users. The common denominator and characteristic feature of all cyber crime offences and cyber crime investigation can be found intheir relation to computer systems, computer networks and computer data on the one hand and to cyber systems, cyber networksand cyber data on the other hand. Cyber crime covers offenses concerning traditional computers as well as cloud cyber space andcyber databases.

National rapporteurs can contact the general rapporteur in case of further inquiries or questions: Prof. Dr. Thomas Weigend:

thomas.weigend@uni-koeln.de

(B) Criminalisation

Please note that in this questionnaire only general characteristics of cyber crime offense definitions are of interest. Specific questionsof individual crime definitions will be discussed in Section II of the Congress.

(1) Which specific legal interests are deemed to be in need of protection by criminal law (e.g., integrity of data processing systems,privacy of stored data)?

It is possible to identify two main categories. First: traditional legal interests protected against new forms of crimes or criminal activities; second: new legal interests.

The first category may include:

1. Property or integrity of computer data, software and systems: art. 640 terc.p. (computer fraud); art. 615 quinquiesc.p. (Dissemination of software or tools designed to damage or interrupt a computer system / data interference); 635 bis (damage and of information, data and software / data interference), 635 ter(damage, of information, data and software of public utility and/or of the State / data interference), 635 quater (damage of computer system / data interference), art. 635quinquies(damage of computer system of public utility and or of the State / data interference).
2. „Public trust" in the payment instruments (art. 55.9, Dlgs 231/2007: abuse of credit/debit cards)

* Prof. Carlenrico PALIERO, University of Milan; in cooperation with Lorenzo Picotti, Roberto Flor, Ivan Salvadori – University of Verona.

3. Public trust and confidence (art. 491 bisc.p. – computer related forgery; 495 bisc.p. - False declarationorstatement for thecertificationofelectronic signatureor about the identity; 640 quaterc.p. – computer fraud committed by anyone who certificates the electronic signature).
4. Secret (art. 621 c.p.)
5. Intellectual Property Rights (in particular copyright: criminal offences provided by L. 633/41)

The second category may include:

1. Right to respect for private life in the form of right to informational self-determination, privacy (criminal offences provided by Dlgs 196/2003), integrity and security of computer data and systems (art. 615 terc.p. – illegal access; art. 615 quaterc.p. – Misuse of device; art. 617 quater, quinquies and sexies – related to illegal interception of non-public transmissions of computer data to, from or within a computer system)
2. Iusexcludendialios with regard to illegal access to work protected by copyright law (violation of technological protection measures).

(2) Please give typical examples of criminal laws concerning

(a) attacks against IT systems and data:

a.1: Criminal laws concerning illegal data interference:

Art. 635-bis of the Italian Penal Code criminalizes "whoever destroys, damages, deletes, alters, or suppress information, programs or computer data of others. The perpetrator is punished with imprisonment from 6 months to 3 years.

Art. 635-ter, paragraph 1, of the Italian Penal Code criminalizes the acts directed to destroy, damage, delete, alter or suppress information, programs or computer data used by the State or other public body or computer data that have however public utility. The perpetrator is punished with imprisonment from 1 year to 4 years.

Art. 635-ter, paragraph 2, of the Italian Penal Code: The perpetrator is punished with imprisonment from 3 years to 8 years if from the act results information, programs or computer data destruction, damage, alteration or suppression.

a.2: Criminal laws concerning illegal systems interference:

Art. 635-quarter, paragraph 1, of the Italian Penal Code criminalizes: "whoever, by the acts of art. 635-bis penal Code, or by imputing or transmitting data, information or programs, destroys, damages, renders, totally or partially useless or seriously hinders the functioning of information systems. The perpetrator is punished with imprisonment from 1 year to 5 years.

Art. 635-quinquies of the Italian Penal Code criminalizes: "the acts of art. 635-quater directed to destroy, damage, render, totally or partially useless an information system of public utility or to seriously hinder its functioning. The perpetrator is punished with imprisonment from 1 year to 4 years.

Art. 635-quarter, paragraph 2, of the Italian Penal Code: " The perpetrator is punished with imprisonment from 3 years to 8 years if from the act results the destruction or damaging of an information system of public utility or if the information system is totally or partially rendered useless.

(b) violation of IT privacy and secret:

Art. 615 terc.p. criminalizes the illegal access to computer system or permanence in a computer system protected by security measures (penalties: imprisonment of up to 3 years)

Art. 617-quater, paragraph 1, of Italian Penal Code criminalizes "whoever intercepts communications relating to an information system or transmitted among more information systems or otherwise hinder or or interrupt such communications. The perpetrator is punished with imprisonment from 6 months to 4 years.

Art. 617-quater, paragraph 1, of Italian Penal Code criminalizes, with the same punishment of art. 617-quater, paragraph 1, whoever totally or partially discloses through any information media the content of such communications.

Art. 617-quinquies of Italian Penal Code criminalizes "whoever, without any law permission, installs devices able to intercept, obstruct or interrupt communications between information systems or transmitted among more information systems". The perpetrator is punished with imprisonment from 1 year to 4 years.

Art. 617-sexies of the Italian Penal Code criminalizes "whoever with the intent to procure for himself or for others an advantage or to cause a damage to others totally falsifies, alters or deletes totally or partially the content, even if occasionally intercepted, of the communications relating to an information system or transmitted among more information systems. The perpetrator is punished if uses these communications or let that other use them with imprisonment from 1 year to 4 years.

Art. 621 of the Italian Penal Code criminalizes whoever having learnt the content, that must be remain secret, of data, information or programs stored in a public or private computer document of others, discoloses, without right, or uses it for his or other's people profit. If the illegal act causes a damage, the perpetrator is punished with imprisonment up to 3 years or with a fine from 103 to 1.032 euros.

Art. 167 Privacy Act (*Unlawful Data Processing)*

1. Any person who, with a view to gain for himself or another or with intent to cause harm to another, processes personal data in breach of Sections 18, 19, 23, 123, 126 and 130 or else of the provision made further to Section 129 shall be punished, if harm is caused, by imprisonment for between six and eighteen months or, if the offence consists in data communication or dissemination, by imprisonment for between six and twenty-four months, unless the offence is more serious.

2. Any person who, with a view to gain for himself or another or with intent to cause harm to another, processes personal data in breach of Sections 17, 20, 21, 22(8) and (11), 25, 26, 27, and 45 shall be punished by imprisonment for between one and three years if harm is caused, unless the offence is more serious.

(c) forgery and manipulation of digitally stored data:

According to art. 491-bis of Italian Penal Code the punishments provided for the forgery crimes are must be enforced also to the forgery concerning public or private electronic document having effects/value of evidence.

Art. 640- ter of Italian Penal Code ("Computer fraud) criminalizes "whoever, altering in any way the functioning of an information system or manipulating without right data, information or programs stored in an information system, gains

an unlawful profit with a damage for other. The perpetrator is punished with the imprisonment from 6 months to 3 years and the fine from 51 to 1.032 euros.

(d) distribution of computer viruses:

Art. 615-quinquies Italian Penal Code criminalizes "whoever, with the intent to damage illicitly an information or telecommunication system, the information, the computer data or programs stored in an information system, or to favour the total or partial interruption or the alteration of its functioning, procures for himself, produces, reproduce, imports, spreads, communicates, delivers, or otherwise makes available to others equipment, devices or programs. The perpetrator is punished with imprisonment up to 2 years and the fine up to 10.329 euros.

(e) crimes related to virtual identities of users, e.g., forging, stealing or damaging virtual personalities

It doesn't exist specific criminal offences. With regard to ID related fraud, identity theft or phishing it is possible to apply different criminal provisions, such as art. 494 c.p. – Impersonation; art. 640 – Fraud; art. 615 quaterc.p. – Misuse of device)

(f) other innovative criminal prohibitions in the area of ICT and internet, e.g., criminalisation of the creation and possession of certain virtual images, violation of copyright in the virtual sphere.

Art. 615-quater of Italian Penal code Criminalizes "whoever with the intent to procure for himself or for others a profit or to cause a damage to others, without right procures for himself, reproduces, spreads, communicates an access code, password or other devices able to access to an information system protected by security measures or otherwise provides information or instruction able to this scope. The perpetrator is punished with imprisonment up to 1 year and the fine up to 5.164 euros.

Art. 600-quater of Italian Penal code Criminalizes "whoever procures for himself or possess pornographic material created using a minor under 18 years of age. The perpetrator is punished with the imprisonment up to 3 years or and a fine non inferior to 1.549 euros.

According to Art. 600-quater.1 ("virtual child-pornography) of Italian Penal code, art. 600-quater is applicable also when the pornographic material represents virtual images realized using minors under 18 years of age or a part of them. In this case the punishment is decreased of 1/3.

About the copyright infringement, art. 171, a) bis, and 171.2 ter, a) bis, L. 633/41 provide as criminal offence the diffusion or communication, through the illegal upload in Internet, of works protected by copyright.

Among the phenomenon "file sharing" only the "upload" is criminalized.

(3) How is criminal conduct (actusreus) typically defined in these crimes (by description of act, by consequence, other)? How is theobject defined ("data", "writings", contents)?

About actus reus, the conduct is not defined but the legislator has criminalized different conduct with different meaning, such as:

altering in any way the functioning of an information system or manipulating without right data, information, interception, interruption, damage, produces, reproduce, imports, spreads, communicates, delivers, or otherwise makes available, diffusion, detention, procure, access, permanence, destroys, renders, totally or partially useless or seriously hinders the functioning of information systems, process.

About copyright infringement the structure of the criminal offences is based on the specializing element of the conduct: "connection in Internet" and, in particular, "upload" of whole or any part of a work without right.

The object is defined as:

Data, information, software/program, computer system (public or private), electronic document, access code, devices able to access, devices able to intercept, obstruct or interrupt communications, virtual (child pornography) image.

About criminal copyright infringement, the object is defined as "work protected by copyright". The reference is to L. 633/41 (copyright act). It may include also movies, music and/or video distributed in Internet, online contents protected by copyright, software and data bases.

(4) Is criminal liability for certain cyber crime limited to particular groups of perpetrators and/or victims?

No. Some provisions of the Privacy Act are applied to: Data controller, Persons in Charge of the Processing, Data processor.

(5) Does criminal liability in the area of ICT and internet extend to merely reckless or negligent conduct?

About negligent conduct there is only one case: omission in the adoption of security measures, provided by the Law-Decree (Decreto legislativo) 196/2003 (Privacy Act).

Art. 169 provides a *misdemeanor* with the penalty of arrest (for up to two years) for the omission in the adoption of minimum security measures referred to the Privacy Act.

At mens rea level, about reckless conduct, the structure of many criminal offences (which provide the "dolo generico" – willful) is compatible with dolus eventualis, using the elastic formula of the acceptance of the risk which requires two elements:

1. Representation: consciousness of the concrete possibility or probabilityof the event/fact
2. Volition: the acceptance of the risk.

(I.e. Illegal access to computer system accepting the risk to violate the contractual limits on the access to the system).

(6) Are there specific differences between the definition of cyber crimes and "traditional" crimes?

It is possible to distinguish two levels: 1. phenomenological and 2. juridical.

1.

The advent of the Internet has brought substantial changes: at phenomenal level, the dissemination of illegal contents (IP infringements, child pornography, incitement to racism and xenophobia, ect.), illegal access to computer systems (through the Internet), system and data interference, illegal interception of non-public transmissions of computer data, new communication tools also useful for the preparation of serious crimes (such as terrorism. See U. Sieber., P. Brunst, *Cyberterrorismand Other Use of the Internet for Terrorist Purposes – Threat Analysis and Evaluation of International Conventions,* inCouncil of Europe (ed.), *Cyberterrorism – the use of the Internet for terrorist purposes,* Strasbourg, Council of Europe Publishing, 2007.

The worldwide proliferation of Information and Communication Technologies has facilitated the commission and the preparation of these types of "criminal activities", which pose threats not only to the confidentiality, integrity or

availability of computer systems and data and to the security of "critical" infrastructures, but also to the Intellectual Property rights, property and public confidence.

At the terminological level, the terms "Internet-crime" and "Cybercrime" have increasingly been used (see U. Sieber, *Mastering Complexity in the Global Cyberspace: The Harmonization of Computer-Related Criminal Law,* in M. Delmas-Marty, M. Pieth, U. Sieber, (eds), *Les chemins de l'HarmonisationPénale/Harmonising Criminal Law, Collection de L'UMR de DroitComparé de Paris, Bd. 15.* Paris, Société de législationcomparée, 2008, 127 – 202).

The offence conduct characterizing the category "cybercrime" includes not only specific computer related crime, but also the use of the new technologies and Internet to commit a wide variety of "traditional" crimes which may be committed also "through means other than by the use of a computer" (See M. F. Weismann, *International Cybercrime: Recent Developments in the Law*, in R. D. Clifford (ed.), *Cybercrime*, III Ed., Carolina Academic Press, 2011, 257, 258).

In general cybercrimes are often divided into three categories: crimes in which the computer (and, in general, new technologies and Internet) are a tool used to commit a crime; crimes in which the computer system is the target of the criminal activities; crimes in which the use of the new technologies and the Internet is an "incidental aspect" of the commission of the crime (See S. W. Brenner, *Defining Cybercrime: A Review of Federal and State Law*, in R. D. Clifford (ed.), *Cybercrime*, cit., 15-104, 17). In other words, they play a non-essential role in the commission of the offence and the computer could be a source of evidence.

2.

In Italy at juridical level, with reference to the structure of the criminal offence, Authors distinguish between

a. "Computer crime in the narrow sense": computer and, in general, new technologies is/are an essential element, or the computer, or information stored on the computer, is/are the subject or target of the criminal activities
b. "Computer crime in the broader sense" : new technologies are not an essential element in the structure of the criminal offences, but could be a tool used to commit a crime, or are the environment or context (see L. Picotti, La nozione di "criminalitàinformatica" e la suarilevanza per le competenzepenalieuropee, in Rivistatrimestraledirittopenaleeconomia, Nr. 4, 2011, p. 827).
c. Cybercrime in the narrow sense: Internet or the connection are an essential element in the structure of the offence (i.e. lett. a) bis art. 171 and 171 ter L. 633/41)
d. Cybercrime in in the broader sense: Internet or the connection are not an essential element in the structure of the criminal offences, but could be a tool used to commit a crime, or are the environment or context
e. At last, Information and Communication Technologies has facilitated the commission and the preparation of these types of "criminal activities". In this case, with reference to the "preparatory acts", the use of the new technologies and the Internet is an "incidental aspect" of the commission of the crime.

Thisconceptual differencehas been elaboratedby the doctrine also on the basis of the Cybercrime Convention, which provides that each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures for the purpose of specific criminal investigations or proceedings and shall apply these powers also to the collection of evidence in electronic form of a criminal offence.

The scope of Section 2 of Chapter II (procedural law issues) of the Convention goes beyond the offences defined in Section 1 in that it applies to any offence committed by means of a computer system or the evidence of which is in electronic form.

(C) Legislative technique

(1) Are there specific problems with respect to the principle of legality (e.g., vagueness, open-ended reference of the crime definitionto other regulations)?

The main problems concerning the Italian cybercrime legislation are:

a. the legislative technique used by the legislator. The cybercrime offences are sometimes characterized for the anticipation of the criminal protection of the legal interest (Rechtsgut") such as the confidentiality, integrity and availability of computer data and systems. See for example the "delicte-obstacle" of art. 615-quater (unauthorized detention and diffusion of access codes to information systems), art. 615-quinquies (diffusion of malware) and the "attempt or inchoates-offences" ("delitti di attentato"/Unternehmensdelikte) of the art. 635-ter and art- 635-quinquies of the Italian Penal Code.
b. Use of terms without legal definition (i.e. "security measures").
c. "Indeterminate" criminal offence: to define the precept / rule it is necessary the reference to the civil and administrative law (i.e. "electronic document" or illegal processe of personal data).

(2) How does legislation avoid undue chilling effects on legitimate use of ICT or of the internet?

In some offences the mensrea requires a specific illegal intent ("dolospecifico") in order to delimitate the illegal acts. See for example art. 615-quaterc.p. (unauthorized detention and diffusion of access codes to information systems) requires that the perpetrator realizes the illegal act with the intent to procure for himself or for others a profit or to cause a damage to others,or art. 615-quinquies (diffusion of malware) that requires that perpetrator realizes the conduct with the intent to damage illicitly an information or telecommunication system, the information, the computer data or programs stored in an information system. Some offences requires that the perpetrator realizes the illegal conduct without authorization ("abusivamente") , such as in art. 615-ter c.p., or without right ("fuoridaicasiconsentiti dalla legge): see, e.g., art. 617-quinquies c.p.

(3) How does criminal legislation avoid becoming obsolete in light of rapid technological innovation? E.g.

Sometimes the legislator used technology-neutral language so that the cybercrime offences may be applied to both current and future technological innovation. See for example the concepts of computer data, security measure (ex art. 615 terc.p.), information system.They are not defined by the legislation.

The Privacy Act defines the security measure for the processing of personal data. In this case the risk is the violation of the principle of legality, because the definition and the implemention of the measures are left to protocols or administrative acts.

- how are changes in the use of internet and social networks taken into account?

Actually these changes are not yet taken into account by the Italian criminal legislator due to the fact that the cybercrime legislation has been introduced in 1993, when the social networks were not yet known. The reforms introduced with the law 48/2008 in order to implement at national level the Cybercrime Convention have not been taken partly into account the changes in the use of social network. Some criminal offences (i.e. cybercrime in the the

broader sense) are applicable. Nevertheless in the case law has emerged, e.g., the legal gap concerning the criminal liability of the director of electronic newspaper or responsible of social network for the illegal contents published on these new media.

- how is the law adapted to technological progress (e.g., by reference to administrative regulations)?

In order to adapt cybercrime legislation to technological progress the Italian legislator normally introduces new laws. See paradigmatically the reform of data and system interference offences introduced by law n. 48/2008. The reference to administrative regulations is used in specific areas (i.e. Privacy Act, on the technical protection measuresto adaptto technological progress)

(D) Extent of criminalization

(1) To what extent do criminal laws cover mere preparatory acts that carry a risk of furthering abuse, e.g., acquisition or possession of software that can be used for "hacking", "phishing", computer fraud, or bypassing download protection? If so, has there been controversy about introducing such laws? Have legislatures made specific efforts to avoid over-criminalization?

The Italian Criminal Information Law criminalizes some preparatory acts, such as the preparatory acts to the illegal access to an information system (art. 615-*ter*c.p.), to computer damage (arts. 635-*ter* and art. 615-*quinquies*c.p.), to the data interception, illegal hindering and interruption of telecommunication (art. 617-*quater*c.p.). The Italian legislator did not avoid through the law n. 547/1993 (see the crimes quoted in paragraphs (i), (ii) and (iii) and the recent law 48/2008 (see the paragraph (IV) a over criminalization in the field of cybercrime. In fact the preparatory act is considered as an independent criminal offence and it is not considered as a part or step of another offence.

A paradigmatic example of preparatory acts is the art. 615-*quater*c.p. (Illegal detention and diffusion of access codes to information systems"). It criminalizes whoever with the intent to procure for himself or for others a profit or to cause a damage to others, without right procures for himself, reproduces, spreads, communicates an access code, password or other devices able to access to an information system protected by security measures or otherwise provides information or instruction able to this scope. The perpetrator is punished with imprisonment up to 1 year and the fine up to 5.164 euros.

Art. 615-*quater*c.p. criminalizes an indirect danger (crime of indirect danger, "reato di pericoloindiretto") and in some cases a double indirect danger (crime of a double indirect danger, "pericolo doppiamente indiretto"). It criminalizes the risk of an illegal access to an information system (a danger for the confidentiality of the data contained into an information system) and the risk of the diffusion of access codes with future acts of illegal access or diffusion. This offence anticipates too much the protection of the legal good and it is not in line with the principle of proportionality, that is very important to analyze the constitutional legitimacy of crime of indirect danger ("reati di pericoloindiretto").

(ii) Another example of preparatory act is represented by art. 615-*quinquies*c.p. (Dissemination of devices or computer programs directed to damage or hinder an information system). It criminalizes whoever, with the intent to damage illicitly an information or telecommunication system, the information, the computer data or programs stored in an information system, or to facilitate the total or partial interruption or the alteration of its functioning, procures for himself, produces, reproduce, imports, spreads, communicates, delivers, or otherwise makes available to others equipment, devices or programs. The perpetrator is punished with imprisonment up to 2 years and the fine up to 10.329 euros.

Art. 615-*quinquies*c.p. criminalizes those acts that aim to gain for himself or another person malware programs that are instrumental to the commission of a system interference offence (art. 635-bis c.p.). According to the scholars, art. 615-*quinquies*c.p. is a crime of eventually indirect danger ("reato di pericoloeventualmenteindiretto"). Getting the availability of a malware can be finalized to the introduction of this program into an information system, or a second diffusion of the program to a third party.

Art. 615-*quinquies*c.p. seems to be in line with the constitutional principle of proportionality since it protects the legal goods of the integrity and correct functioning of the information systems and it criminalizes acts that represent a risk for these legal interests.

(iii) Another offence having the structure of a preparatory act, even if it does not criminalize only preparatory acts, is represented by art. 617-*quinquies*c.p. It criminalizes whoever, without any law permission, installs devices able to intercept, obstruct or interrupt communications between information systems or transmitted among more information systems". The perpetrator is punished with imprisonment from 1 year to 4 years. It is a concrete dangeroffence ("reato di pericolo concreto"). The object of the crime is represented by devices able to intercept, obstruct or interrupt communications between information systems or transmitted among more information systems (i.e. exploiting the telephonic connection or intercepting the data flow).

(iv) In the field of the computer damage offences, the Italian legislator has introduced (with the law 48/2008) two new offences, structured on the model of an attempt-crime (inchoate-offence: "reati di attentato"/Unternehmensdelikt). The act is directed to damage "information, programs or computer data used by the State or other public body or computer data that have however public utility" (art. 635-*ter* c.p.) or information system of public utility (art. 635-*quinquies*c.p.). Art. 635-*ter* and art. 635-*quinquies*c.p. criminalize "acts directed to destroy" but not the real destruction of information, data and programs. Their structures is similar to art. 420 c.p. (Attempt to an installation of public utility, "Attentato ad impianti di pubblicautilitá").

The scholars have criticized the structure of art. 635-*ter* and art. 635-*quinquies*c.p. that anticipate the penal protection because in this case there are not the reason that justify the use of an attempt-crime ("reato di attentato") structure.

(2) To what extent has the mere possession of certain data been criminalized? In what areas, and on what grounds? How is "possession" of data defined? Does the definition include temporary possession or mere viewing?

The mere possession of certain data is criminalized in three cases concerning two different areas. The first area concerns cases of cybercrime in a wide meaning, according to the definition of point B.6 of this questionnaire: arts. 615-*quater*c.p. (illegal detention or diffusion of access code to an information system) and art. 615-*quinquies*c.p. (diffusion of devices or tools directed to damage or hinder an information system). The second area concerns computer crimes in a wide meaning: art. 600-*quater* (detention of child pornography) or possession of virtual child pornography (art. 600-*quater.*1 c.p.). The acts criminalized in these offences have been already analyzed before in the points B.2 and D.1.

(I) Art. 615-*quater*c.p. criminalizes the possession of access codes to an information system. The offence anticipates the protection of art. 615-*ter*c.p., concerning the illegal access to an information system. In order to limit the excessive anticipation of the penal protection, the offence criminalizes only the possession of access codes with the intent to gain a profit or to cause a damage. The possession is a consequence of the act of acquirement codes,

password or other devices adapted to access to an information system by a person that is not authorized to use them. Therefore the possession requires a previous act of acquirement tools in order to access to an information system. The mere acquirement without a positive act of the perpetrator is not illegal.

(ii) Art. 615-*quinquies*c.p. criminalizes the possession of programs directed to damage or hinder an information system. The aim of the offence is to create an obstacle to the commission of the computer damage offences (art. 635-*bis*c.p., art. 635-*quinquies*c.p.). The offence criminalizes only the possession with the intent to damage an information system. In line with art. 615-*quater*c.p., the concept of possession of the art. 615-*quater*c.p. comes from the act of acquirement codes, password or other tools designed to access to an information system. Nevertheless art. 615-*quinquies*c.p. criminalizes not only the possession but also the production of access codes and password, even if these tools are not been acquired by the perpetrator but produced by himself.

(iii) Art. 600-*quater*c.p. criminalizes the detention and the procurement of child pornography and anticipates the penal protection provided for art. 600-*ter*c.p., criminalizing the production, the commerce, the cession and the diffusion of child pornography. The offence does not require a specific intent ("dolospecifico") but requires that the acts is committed "consciously"/ "knowledge" ("consapevolmente"), excluding the doluseventualis ("doloeventuale"). The detention of child pornography exists when the perpetrator downloads into his computer child pornography files. This offence does not criminalize the mere visualization or access to child pornography through information and communication technologies. Therefore art. 600-*quater*c.p. does not criminalizes the temporary possession or the visualization of such material.

(3) To the extent that possession of or granting access to certain data have been defined as criminal, does criminal liability extend to service providers (e.g., hosting or access providers)? What are the requirements of their liability, especially concerning mens rea? Are providers obliged to monitor and control what information they provide or offer access to? Are providers obliged to provide information on the identity of users? Are providers obliged to prevent access to certain information? If so, under what conditions, and at whose cost? Is there criminal liability for violating such obligations?

The Italian Law has gaps about the ISP liability and doctrine and jurisprudence call for a legislative intervention.

Courts follow the interpretation that ISP is not responsible for criminal offences committed by users who upload or possess illegal content and there are 5 areas where it is possible to support the accountability/liability of ISP:

Child-pornography;

Defamation (in particular in or through Social Networks);

Criminal copyright infringement;

Economic crimes (dissemination of false financial information);

Privacy protection.

With regard to Privacy protection and criminal privacy infringement, one of the most famous judgements about Internet and Criminal Law is the decision of the Tribunal of Milan of 2010 (Google vsVivi Down)

The decision shows the absence of a specific law about the ISP liability for criminal offences committed by users and, in particular of a position of guarantor, due to impossibility of a control on the contents uploaded online.

But the judge admits the breach of obligations provided by the Privacy Act (D.lgs. 196/2003) by the ISP and the liability of the ISP as contributor to the crime (art. 167 Privacy Act, unlawful processing of data) with the user/author

The ISP is the perpetrator, as data controller, because it did not inform users about their duties and obligations for the processing of sensitive data

This case law solution shows the gaps of the law.

First, it can not be extended to other criminal offences, in particular in cases without a specific civil or administrative law/regulation.

Therefore it does not extend to the other four areas

Second, the solution is a misunderstanding: it defines the criminal liability for a commissive fact but using the language of an omission, because the conduct consists of violation of certain obligations, with regard to the position of the ISP.

Third, it is difficult to prove the subjective element (mens rea) of the ISP, which does not have the possibility to know the content of the material uploaded before the upload.

For this reason the judge had to prove at least the dolus eventualis: deliberate non-compliance with the internal rules of the legal person in relation to the process of personal data

In conclusion, it is possible to exclude a position of guarantor for the ISP, in the absence of a specific incrimination by the law.

The ISP may be responsible for a contribution/participation to the criminal offences committed by other (users) as long as there is a specific provision by law that imposes mandatory obligations of conduct.

This solution can be proved to the contrary, with reference to the criminal offences against the honor and reputation committed through Internet: the Italian Supreme Court excluded the criminal liability of the ISP, both for commission and omission.

(4) What general, in particular constitutional limits to criminalizing conduct have been discussed with respect to ICT and internet crime (e.g., freedom of speech, freedom of the press, freedom of association, privacy, "harm principle", requirement of an act, mensrea requirements)?

Among the general principles we have to include the right to privacy (protection of personal data), freedom of expression (freedom to receive or impart information) and freedom to conduct a business

Recently the Court of Justice of the EU ("SABAM v. Scarlet Extended SA", 24 Nov. 2011) stated that an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right', to order an [ISP] to install, for all its customers, in abstracto and as a preventive measure, exclusively at the cost of that ISP and for an unlimited period, a system for filtering all electronic communications, both incoming and outgoing, passing via its services, in particular those involving the use of peer-to-peer software, in order to identify on its network the movement of electronic files containing a musical, cinematographic or audio-visual work in respect of which the applicant claims to hold rights, and subsequently to block the transfer of such files may infringe the fundamental rights of that ISP's customers, namely their right to protection of their personal data and their freedom to receive or impart information, which are rights safeguarded by Articles 8 and 11 of the Charter respectively (and artt. 8 e 10 ECHR) and the freedom to conduct a business (art. 16 of the Charter).

The same principle was applied also in the case "SABAM v. Netlog NV" (Court of Justice, 16 Feb. 2012).

It must be held that the injunction to install the contested filtering system is to be regarded as not respecting the requirement that a fair balance be struck between, on the one hand, the protection of the intellectual-property right enjoyed by copyright holders, and, on the other hand, that of the freedom to conduct business enjoyed by operators such as hosting service providers.

With these decisions the Court of Justice emphasized the fundamental rights that can find expression in cyberspace in comparison to the need to protect intellectual property in Internet

At national level the principle of legality (art. 25 Cost.) hindered that specific conducts committed through ICTs were criminalized on the basis of traditional criminal offences.

For example, before the entry into force of art. 635 bis p.c. doctrine denied the possibility of applying the traditional offence of damage of material things to the software sabotage, because data and software are intangible (goods), not related to the notion of "thing". To extend criminalization, at the level of interpretation, was a violation of prohibition of analogia in malam partem.

Similarly, the provision of computer related fraud (art. 640 ter p.c.) is justified by the difficulty of applying the "traditional" fraud for conducts punished by art. 640 ter, that do not include the element of deception/error of the person/victim.

The principle of strict legality is a limit of criminal law also in the matter of on-line newspapers.

Doctrine and jurisprudence have debated (and are currently debating) whether the editor or the director of an on-line newspaper is responsible for the criminal offences committed by the journalists and/or users (art. 57 p.c.): for example for defamation, violation of secrets, frauds, obscene publications, unlawful processing of personal data, in particular when the newspaper is the instrument used for the violation of a legal interest.

Some Authors deny the applicability of laws about traditional newspapers to on-line newspapers, on the basis of L. 47/1948: the notion of "printed" does not include the online instruments.

Art. 6 CoC criminalizes preparatory acts and its formulation creates problems. The national legislators had to select in detail the facts to be punished, with specific and limited elements (both at actus reus and mens rea level)

The Italian Law 48/2008, which implemented the Cybercrime Convention, reformulated art. 615 quinquies p.c., which criminalizes preparatory acts: legal and usual conducts in the Information Society that become harmful or dangerous for the intent of the perpetrator

Law 38/2006 (provisions on the fight against child pornography in Internet, sexual abuse and sexual exploitation of children), provided arts. 600 ter and 600 quater p.c.

For the purpose of art. 9.1. CoC, the term "child pornography" shall include pornographic material that visually depicts: a) a minor engaged in sexually explicit conduct; b) a person appearing to be a minor engaged in sexually explicit conduct; c) realistic images representing a minor engaged in sexually explicit conduct.

Some Authors claim that the new law violates the general principles of criminal law, even if it responds to the need to protect children in Internet. It is, for these Authors, a *victimless crime:* it doesn't exist a real victim and the criminalization and the perspective of protection of the legal interest is based on the intent of the perpetrator, in

violation of the principles of "materiality" and "precision", proportion and rehabilitation of the penalty (for the severity of the penalties).

Creating crimes without victims or without offence is common in the field of computer crimes.

The question is focused on the use of new technologies or, in other words, if it constitutes new forms of aggression of traditional or well known legal interests or if it created one new common legal interest worthy of an independent criminal protection.

Often it consists of new forms of aggression, even if new technologies are, in some cases, elements of the criminal offence. It shown by the "location" of the new criminal offences for the protection of traditional legal interests, in different parts of the criminal code and special laws.

The notion of legal interest limits the criminal law area only if connected to general principles, which go be beyond the positive legal system:

Prohibition to criminalize the legal exercise of constitutional rights;

Obligation of secularism of the legal system.

In subiecta materia the notion of legal interest has not limited the use of criminal law. On the contrary, it has encouraged the use of criminal law

The needs of protection of the "risk society" has determined political choices in criminal law matter and, in particular, in the area of cyber crime, that have created artificial and immaterial legal interests.

(5) Does the law provide for criminal sanctions specifically targeting cyber criminals (e.g., a temporary ban from using the internet)?

No. The Italian legal system doesn't provide specific penalties for cyber-perpetrators/criminals. But the law 15th February 2012 number 12 provide a new special case of confiscation of computer and electronic devices used by cyber- and computer-criminals.

(E) Alternatives to Criminalization

(1) What role does criminal law play in relation to other ways of combatting abuse of ICT and the internet? What is the relationship of civil and administrative sanctions (payment of damages, closing of enterprise, etc.) to criminal sanctions in the area of ICT?

According to a systematic fundamental principle, in our legal system a criminal offence must be a civil offence at the same time. In fact in the criminal law the criminal sanction is used to strengthen the comply of a precept belonging not only to the criminal law but also to all legal system. A civil offense can be not a criminal offence, but a criminal offence always constitutes a civil offence.

Therefore an illicit act committed through the information and communication technologies can be punished as civil offence according to art. 2043 of the Italian Civil Code (c.c.), even if it is not constitute a criminal offence too. According to our jurisprudence (see i.e. our Court of Cassation) the right to the legal reparation of the civil damage requires that the illicit act has caused a damage. Art. 2043 c.c. requires the following elements: an act, the mens rea (at least the negligence), a causal nexus and a result of a juridical position deserving of protection into the legal system.

At one with these principles, the civil responsibility has been recognized respect to Google Inc. for a defamation automatically caused by a software. A businessman discovered that including his name and surname into the Google "suggest search" service the software suggested the following words: "fraud" and "swindler". According to the businessman association between his name and "swindler" was not only false but also defamatory, representing an offence to his honor, his image and his personal and professional reputation. Appealing to the extra-contractual responsibility (aquilian liability) of Google on the basis of art. 2043 c.c. he required to the Italian Court to impose to Google Inc. the removal into the Google suggest search service the association between his name and the word "swindler". The businessman required a compensation to Google Inc. for each day late in fulfillment of the court order. According to the businessman Google had the juridical obligation to stop the defamation to his honor and reputation caused through its services.

The mens rea of the Italian defamation offence requires dolus generalis such as the will to use offensive expressions with the consciousness to offend the reputation of a person. In the case already mentioned, the association between the name of the businessman and the words "fraud" and "swindler" was automatically produced by a software. For this reason there were not any dolus generalis, as required by the criminal defamation offense. Nevertheless in a civil process is not necessary to prove the dolus generalis. The aquilian liability requires only to prove the negligence.

An illicit offence committed through information and communication technologies, infringing the general principle of "neminem laedere", legitimates only the injured to require a compensation for the prejudice, even if the act is not a criminal offence.

On contrary, in this field of information and communication technologies abuses the relationship between criminal and administrative sanctions is very limited. Normally it is possible to apply an administrative sanction when the act is not a crime (see i.e. art. 12 d.lgs.70/2003).

(2) What non-criminal means of combatting offensive websites are used/propagated (e.g., closing down websites, blocking access to websites)?

A non-criminal means of combatting offensive websites is the adoption of a private internet filtering system of the contents. There are two different approaches in order to block access to websites: using a blocking system of the negative contents; accepting only the positive contents. The first solution consists of blocking access to specific web pages, creating a black list of webpages that are not suitable for some users (list of banned webpages). The second solution consists of creating a list of permitted webpages, according to the model of a home library or walled garden.

These systems are named parental control because they are used above all by families in order to avoid that their children can take contact with illegal and dangerous contents. Similar systems are used also by the enterprises. Due to the impossibility to control the netsurfing of the employers, the enterprises need a filtration system in order to limit the access to webpages that are not strictly related to the professional activities (pornography, gambles, games, etc.).

Other the means directed to prevent the commission of abuses on line, it is also possible to act ex post in order to stop an abuse already committed. If a user considers that someone has gained without access to his email can report the event to the Internet Service Provider. The ISP's make available to the users an email address in order to report the abuses. Also the Social network and the blogs give to the users the possibility to report the abuses committed through the information and communication technologies.

The Internet filtering system can be activated also by the authority with a legal injunction directed to the ISP's. Paradigmatic is the case of the Pirate Bay. The Tribunal of Bergamo ("Giudice per le indagini preliminari") blocked the access to this webpage in 2009 in order to avoid the commission of the art. 171-ter, comma 2, lit. a-bis of the Law 22thApril 1941, n. 633. The Court of Cassation has established the legitimacy of the precautionary measure that does not establish only the seizing of an illegal webpage but also that the ISP's have to stop the access to the webpage. The legal decree n. 70/2003 (D.lgs. 9thApril 2003, implementing the European Directive 2000/31/CE) recognizes to the legal authority, to the vigilance authorities and independent authorities a special inhibitory power, infringing the free circulation of access service, for the reasons provided for art. 5 D.lgs. 70/2003: public order (prevention, investigation, individuation).

(3) To what extent are ICT users expected to protect themselves (e.g., by encryption of messages, using passwords, using protective software)? Are there sanctions for not protecting one's computer to a reasonable extent, e.g., by using anti-virus software or protecting access to private networks by password? Does the lack of reasonable self-protection provide a defense for defendants accused of illegally entering or abusing another person's network or abusing their data?

The expectation that users adopt protective measures was implemented by the Italian legislature, at least with art. 615 ter p.c., which punishes the illegal access to computer system.

The computer system is protected by criminal law only if security measures are applied.

The reason is twofold: accountability of potential victims; demonstration of the legal interest protected, to increase the rate of materiality/harmful of the criminal offence.

Role, nature and effectiveness of these security measures are discussed.

Many Authors the security measure is any tool/instrument which selects users authorized to access to the system.

In this sense the *jus excludendi alios* is relevant and any tool, also common, is sufficient for this purpose. It does not express the brocard *vigilantibus iura succurunt,* but the legal interest

Security measures are considered: passwords and user names, but also physical or structural instruments (but not, for example, related to the building).

The protection must be present and it is not necessary that it works or, for the jurisprudence (that has exceeded the previous interpretation), the violation of the measure. This latter approach has changed in the more recent case law.

In any case if the system is not protected it is not possible to apply art. 615 ter p.c.

Art. 615 ter p.c. and the criminal law do not provide penalties in case of failure / omission to adopt security measures.

In this sense the absence of security measures is a useful instrument for the defense and it is not relevant that the measures were not reasonable or appropriate to prevent illegal access

Differently there is not an expectation of self-protection in case of system or data damages, committed after an illegal access.

In effect, the criminal offences provided by art. 635 bis and 635 quater p.c. do not require that the system or data must be protected by security measures.

The damage of system or the system interference committed through an illegal access is a criminal offence independently from the fact that the system was or not protected by security measures. In this sense, the absence of the measures is not an element or argument in favor of the perpetrators.

(F) Limiting anonymity

(1) Are there laws or regulations obliging internet service providers to store users' personal data, including history of internet use?

Can providers be obliged to provide such data to law enforcement agencies?

(2) Are there laws or regulations obliging an internet service provider to register users prior to providing services?

Art. 132 Dlgs 196/2003 (Privacy Act) provides a mandatory data retention, in particular:

1.[Without prejudice to Section 123(2)], telephone traffic data shall be retained by the provider for

twenty-four months as from the date of the communication with a view to detecting and suppressing criminal offences, whereas electronic communications traffic data, except for the contents of communications, shall be retained by the provider for twelve months as from the date of the communication with a view to the same purposes.

1-bis. The data related to unsuccessful calls that are processed on a provisional basis by the providers of publicly available electronic communications services or a public communications network shall be retained for thirty days.

[…]

3. Within the term referred to in paragraph 1, the data may be acquired from the provider by means of a reasoned order issued by the public prosecutor also at the request of defense counsel, the person under investigation, the injured party, or any other private party. Defense counsel for either the defendant or the person under investigation may directly request the provider to make available the data relating to the subscriptions entered into by his/her client according to the arrangements specified in Section 391-quater of the Criminal Procedure Code without prejudice to the requirements set out in Section 8(2), letter f), with regard to incoming phone calls.

[…]

4-ter. The Minister for Home Affairs or the heads of the central offices specializing in computer and/or IT matters from the State Police, the Carabinieri, and the Financial Police as well as the other

entities mentioned in paragraph 1 of section 226 of the implementing, consolidating, and transitional provisions related to the Criminal Procedure Code as per legislative decree no. 271/1989, where delegated by the Minister for Home Affairs, may order IT and/or Internet service providers and operators to retain and protect Internet traffic data, except for contents data, according to the arrangements specified above and for no longer than ninety days, also in connection with requests lodged by foreign investigating authorities, in order to carry out the pre-trial investigations referred to in the said section 226 of the provisions enacted via legislative decree no. 271/1989, or else with a view to the detection and suppression of specific offences. The term referred to in the order in question may be extended, on grounds to be justified, up to six months whilst specific arrangements may be made for keeping the data as well as for ensuring that the data in question are not available to the IT and/or Internet service providers and operators and/or to third parties.

4-quater. Any IT and/or Internet service providers and/or operators that are the subject of the order mentioned in paragraph 4-ter shall comply without delay and forthwith give assurances to the requesting authority as to their compliance. IT and/or Internet service providers and/or operators are required to keep the order at issue confidential along with any activities performed accordingly throughout the period specified by the said authority. Violation of this requirement shall be punished in accordance with section 326 of the Criminal code unless the facts at issue amount to a more serious offence.

4-quinquies. The measures taken under paragraph 4-ter above shall be notified in writing without delay, in any case by forty-eight hours as from service on the addressee(s), to the public prosecutor that is competent for the place of enforcement, who shall endorse them if the relevant preconditions are fulfilled. The measures shall cease to be enforceable if they are not endorsed.

5. Data processing for the purposes referred to in paragraph 1 shall be carried out by complying with the measures and precautions to safeguard data subjects as required under Section 17, which are aimed at ensuring that the retained data fulfill the same quality, security and protection requirements as network data as well as at:

a. providing in all cases for specific systems allowing both computer-based authentication and

authorization of persons in charge of the processing as per Annex B,

[…]

d. laying down technical mechanisms to regularly destroy the data after expiry of the term referred to in paragraph 1.

Providers shall establish internal procedures to meet the requests made in compliance with the provisions that envisage access to users' personal data.

(3) Are there laws or regulations limiting the encryption of files and messages on the internet? Can suspects be forced to disclose passwords they use?

No, there aren't. after the implementation of the Cybercrime Convention (L. 48/2008)cooperation with LEAd isencouraged

(G) Internationalization

(1) Does domestic law apply to data entered into the internet abroad? Is there a requirement of "double criminality" with respect to

entering data from abroad?

According to art. 6 Italian Penal Code ("crimes committed within the Italian territory") the crime committed in Italy is punished by the Italian Law. The crime is valuated as committed within the Italian territory when its action or its omission has been realized totally or partially in Italy, or if the result of the action or omission committed has been carried out in Italy. According to this article, the Italian Law could be applied if the data entered into Internet abroad cause an event ("risultato") within the Italian territory (i.e an attack committed abroad against an information system located within the Italian territory).

A requirement of "double criminality" with respect to entering data from abroad is not required in the case of execution of EU Arrest Warrant and other instruments of international cooperation based on the principle of mutual recognition (Art. 8, letter m) of the Law N. 69 of 2005 implementing the Framework decision 2002/584/JHA).

(2) To what extent has your country's criminal law in the area of ICT and internet been influenced by international legal instruments?

The Italian criminal law in the area of ICT and Internet has been influenced by the regional and international legal instruments and specially by the EU Framework Decisions and the Recommendations and Conventions of the Council of Europe. The Law n. 547/1993 on the computer crime, adopted on 23rd December 1993 by the Italian Parliament, has been influenced by the Recommendation 89 (9) of the Council of Europe. It introduces in the Italian legislation the offences provided in the minimum list of the R (89) 9.

The reform to the Penal Law and Procedure Criminal law in the area of ITC and Internet was first introduced with the Law n. 36/2006 extending the incrimination of child pornography and then with the Law n. 48/2008, adopted on 18th march 2008 by the Italian Parliament, ratifying the Cybercrime Convention of the Council of Europe. Nevertheless it is not completely in line with the guidelines of the Council of Europe.

With the recent Law n. 172/2012, adopted on 1st October 2012 by the Parliament, the Italian legislator has ratified also the Convention of Lanzarote of the Council of Europe, modifying the previous legislation and introducing new crimes (i.e. child-grooming) against the sexual exploitation and sexual abuse of minors in the Penal Code.

(3) Does your country participate in discussions about the harmonization of cybercrime legislation (such as the U.N. intergovernmental expert group on cybercrime)?

Italy has participated in discussion about the harmonization of cybercrime legislation organized by the Council of Europe. Italian representatives of the Interpol Office of Rome, Ministry of Interior and Ministry of Justice have also participated in the U.N. Open-ended intergovernmental expert group on cybercrime.

(H) Future developments

Please indicate current trends of legislation and legal debate in your country concerning ICT and internet crime.

In the governmental agenda there aren't today provision of new law or reform of the broad Italian legislation against the computer- and cybercrime.

But the development of the EU Law that involve also this matter – in particular the Directive 2011/92 against child abuse and child-pornography and the Proposal of new Directive and Regulation in the field of privacy and data protection – will need new national law to implement it.

The legal debate today concerns primarily the question of liability of the ISP for the criminal offences committed through his networks and services, in particular the unlawful conduct in the social networks.