Preparatory Colloquium
24-27 April 2013, Moscow (Russia)
Section II: Information Society and Penal Law

ITALY*

Lorenzo PICOTTI(*)

(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 affects interests associated with the use of information and communication technology (ICT), such as the proper functioning of computer systems 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 in their relation to computer systems, computer networks and computer data on the one hand and to cyber systems, cyber networks and cyber data on the other hand. Cyber crime covers offenses concerning traditional computers as well as cloud cyber space and cyber databases.

National rapporteurs can contact the general rapporteur in case of further inquiries or questions: Prof. Dr. Emilio C. Viano: emilio.viano@gmail.com

(B) Legislative Practices and Legal Concepts

(1) How are criminal laws related to cyber-crimes codified in your country? Are they contained in a unified title or code or are they to be found in various codes or titles? (Please, provide appropriate citations).

(2) What is the impact of judicial decisions on the formulation of criminal law related to cyber-crimes?

(3) To catch up with changing needs and circumstances and to attain new objectives, some laws are subject to frequent amendment. Normally, such amendments take the form of new laws. In certain cases these new laws, instead of simply modifying the parts of the law that need to be changed, present the required amendments into a consolidated text together with all past amendments. This technique is called recasting. Is that how cyber-crime laws are updated and adapted to changed realities in your country? Please provide appropriate references and citations.

The Italian Criminal Code provides many criminal offences (the most important part) in different titles of the code, following the criterion based on the " legal interest protected" (for example computer related fraud – art. 640 ter - in the part "crimes against property", after "fraud" – art. 640 - or illegal access in the part "crimes against the person").

But there are also criminal provisions outside the criminal code (for example provided by the Privacy Act or by the Copyright Act – see infra).

Some judicial decisions have influenced the formulation of criminal law related to cyber-crimes (for example art. 392 criminal code - arbitrary exercise of reasons with violence on "thing": the definition of "thing" includes also data and software - or art. 420 criminal code, now repealed and replaced by the new articles about system and data damage)

Usually new cybercrime laws provide new criminal offences (for example computer related fraud, art. 640 ter cc) or new definition or clauses (for example the definition of mail, including email and any type of electronic communication, art. 616 – violation of mail and correspondence - and 623 bis cc – "other communication")

The main important reforms have been implemented by: L. 547/93 (the first Computer related crime act, which introduced specific criminal provisions); L. 269/98 (on child pornography); L. 38/2006 (on child pornography, which

---

* 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.

(*) Prof. Lorenzo Picotti - University of Verona, in cooperation with Dr. Roberto Flor and Dr. Ivan Salvadori – University of Verona

emended the previous law and some articles in the criminal code); L. 48/2008 (the second computer related crime and cybercrime law, which implemented the Convention on Cybercrime).

(a) Integrity and functionality of the IT system

1. Illegal access and interception of transmission

a. Object – system or data?

Our criminal law criminalizes the illegal access to an information or telematic system and the interception of computer data (communications relating to an information system or transmitted among more information systems).

Art. 615-ter c.p. (unauthorized access to an information or telematic system protected by security measures) criminalizes not only the illegal "introduction" but also the "permanence" into an information or telematic system protected by security measures[1].

Article 617-quater, paragraph 1, Italian Penal Code criminalizes the interception of communications relating to an information system or transmitted among more information systems. **Art. 617-quater, paragraph 2,** of Italian Penal Code criminalizes whoever totally or partially discloses through any information media the content of such communications.

Art. 617-quinquies c.p. criminalizes also whoever installs devices able to intercept, obstruct or interrupt communications between information systems or transmitted among more information systems.

Does your criminal law establish as a criminal offense the serious hindering, without right, of the functioning of a computer and/or electronic system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing information or data from a computer system, software or program?

Yes.

Art. 635-quarter, paragraph 1, of the Italian Penal Code criminalizes: "whoever, by the acts of art. 635-bis penal Code (destruction, deletion, alteration, suppression of information, programs of others), or by imputing or transmitting data, information or programs, destroys, damages, renders, totally or partially useless or seriously hiders 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 the its functioning. The perpetrator is punished with imprisonment from 1 year to 4 years. According to **Art. 635-quinquies, 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. Requirement of infringement of security measures?

Is it a requirement of your criminal law that the hacker conduct the hack of the computer system by using one or more software needed to defeat security measures and gain entry-level or higher level of access?

Art. 615-ter c.p. does not expressly require the violation of security measures. For this reason is not a requirement

[1] Art. 615-ter, paragraph 1, c.p.: "Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni".

of the offence that the hacker (or the insider) conduct to gain the introduction or the permanence into an information or telematic system protected by security measures has been committed by using one or more "hacking tools" or other software to defeat security measures.

The offence does not define the concept of security measures. According to the scholars they could include "logical" or "physical" measures adopted to prevent the illegal introduction or permanence into an information or telematic system.

2. Data and system interference

a. Object – protection of system/hardware/data?

a. Object – protection of system/hardware/data?

Does your criminal law define "computer and/or electronic data"?

No, it doesn't.

In the Italian criminal law there is not a definition of "computer and/or electronic data", such as, for example, in the German Penal Code (§ 202a.2 StGB)

Does this definition include programs or software or similar coding?

No, it doesn't. There is any definition.

If you have a definition, please provide it and the reference to the related paragraphs/articles of your code.

b. Act – destruction/alteration/rendering inaccessible?

i. Does your penal law penalize the unauthorized erasure, alteration, rendering inaccessible, acquiring or other similar interference with information or data from a computer or electronic system or program?

Yes.

Articles 635-bis, 635-ter, 635-quater and 635-quinquies of the Italian Penal Code criminalize the unauthorized erasure, alteration, delation, damage, suppression and the rendering inaccessible private or public information, software, computer data and information systems[2].

[2] **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 criminalizes : 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. **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 hiders 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 the its functioning. The perpetrator is punished with imprisonment from 1 year to 4 years. **Art. 635-quinquies, 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.

These articles do not expressly criminalize the unauthorized acquiring of computer data.

ii. Does your penal law penalize the unauthorized interception of the transmission in any manner or mode of computer or electronic data and/or information?

Yes.

Article 617-quater, paragraph 1, Italian Penal Code criminalizes the interception of communications relating to an information system or transmitted among more information systems. **Art. 617-quater, paragraph 2,** of Italian Penal Code criminalizes whoever totally or partially discloses trough any information media the content of such communications

Art. 617-quinquies criminalizes whoever installs devices able to intercept, obstruct or interrupt communications between information systems or transmitted among more information systems.

Art. 621 of the Italian Penal Code criminalize the unauthorized disclosure data, information or programs stored in a public or private computer[3].

3. Data Forgery

Does your penal law define as a criminal offense the unauthorized input, alteration, deletion or suppression of computer or electronic data resulting in inauthentic data in order to protect the authenticity of the data to be used or acted upon for legal purposes? If you have a definition, please provide it along with the reference to the related paragraphs/articles of your code and/or special statutes.

Art. 491-bis Italian Penal Code extends the application of the traditional material and ideological forgery offences (art. 476 ss. CP) to the illegal acts concerning a private or public information document having an evidential efficacy[4].

b. Act – alteration/deletion? Does your penal law penalize as a criminal offense the unauthorized input, alteration, deletion or suppression of computer or electronic data/information resulting in inauthentic data/information with the intent that it be considered or acted upon for legal purposes as if it were authentic? If yes, please provide the reference to the applicable paragraphs/articles of your code.

Articles. 476, 477 and 478 of the Italian Penal Code criminalize the unauthorized alteration or the totally or partially false creation of documents committed by a funcionary ("pubblico ufficiale"). According to art. 482 CP the same material forgeries are criminalized if they are committed by a private citizen ("privato").

Art. 490 of the Italian Penal Code criminalizes the totally or partially suppression, distruction or hide of a true private

---

[3] **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 2,** of Italian Penal Code criminalizes, with the same punishment of art. 617-quater, paragraph 1, whoever totally or partially discloses trough 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. 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.

[4] Art. 491-bis CP: « s*e alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato avente efficacia probatoria, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private* ».

or public document.

Arts. 479, 480 of the Italian Penal Code criminalizes the ideological forgery ("falsità ideologica") committed by a funcionary ("pubblico ufficiale") carrying out his/her public activities. **Art. 481 CP** criminalizes the ideological forgery committed by a officer attending a service of public necessary carrying out his/her activities.

According to **art. 483 cp** the same ideological forgeries are criminalized if they are committed by a private citizen.

According the **art. 491-bis cp**. all these unuathorized acts are criminalized if they concern a private or public information document having an evidential efficacy.

4. Misuse of Devices

a. Object – type of device?

Does your criminal law criminalize the development of a hacker's "tool kit" or any part of it (e.g. password grabbers and key loggers, blue boxing programs, war-dialers, encryption software, program password crackers, security vulnerability scanners, packet sniffers etc.) for the unauthorized access to computer or electronic systems or transmissions?

Yes.

Article 615-quater of the Italian Penal Code criminalizes the reproduction of some "hacking's tools" (such as access code, password or other devices) able to access to an information system protected by security measures[5]. It criminalizes also the furniture of information or instructions (for example through a web page) for this scope.

Art. 615-quinquies of the Italian Penal Code criminalizes the production, reproduction, import, procurement for himself, the spreading, communication, delivering or making available to others some "hacking's tool kits" (such as equipment, devices or programs) with the intent to damage illicitly computer data or an information system[6].

b. Act – public distribution/transfer to another person?

i. Does your criminal law penalize the unauthorized use of any of the hacker's tools listed above under a?

Article 615-quater of the Italian Penal Code criminalizes the procurement for himself, the spreading, and the communication of some "hacking's tools".

The use of hacker's tools is criminalized if it causes a data or system inteference (arts. 635-bis; 635-ter, 635-quater, 635-quinquies c.p.).

---

[5] **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.

[6] **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.

ii. Does your criminal law penalize the public distribution and/or transfer to other parties of hacked electronic information?

Yes.

Art. 615-quater of the Italian Penal Code criminalizes the spreading and the communication of "hacking's tools", such as access code, password or other devices able to access to an information system protected by security measures or otherwise furnish information or instruction suitable to this aim

c. Possession?

Does your criminal law criminalize the possession of a hacker's "tool kit" or any part of it (e.g. password grabbers and key loggers, blue boxing programs, war-diallers, encryption software, program password crackers, security vulnerability scanners, packet sniffers etc.) for the unauthorized access to computer or electronic systems or transmissions?

Article 615-quinquies of the Penal Code criminalizes "the procurement for himself" of a hacker's "tool kit". The "possession" of a hacker's "tool kit" is not expressely criminalized.

(b) Privacy

1. Violation of Secrecy of Private Data

a. Object – type of private data?

(Note: private data are data that belong to people's private life but do not identify or make it possible to identify a person, e.g., civil status, sexual orientation, health status, buying habits or preferences)

i. **Do your country's laws require that data collectors disclose their information practices before collecting private information from consumers like, for example, which information is used, how it is collected and for what purpose, whether it is shared with others and whether consumers have any control over the disclosure of their private data?**

Yes.

According to **art. 13** of the Law 196/2003 (Information to Data subjects) the data collectors have to disclose their information practices before collecting private information from consumers. In particular they have to give to the consumers the following information:

a) the purposes and modalities of the processing for which the data are intended;

b) the obligatory or voluntary nature of providing the requested data;

c) the consequences if (s)he fails to reply;

d) the entities or categories of entity to whom or which the data may be communicated, or who/which may get to know the data in their capacity as data processors or persons in charge of the processing, and the scope of dissemination of said data;

e) the rights as per Section 7;

f) the identification data concerning the data controller and, where designated, the data controller's representative in

the State's territory pursuant to Section 5 and the data processor[7].

According to **art.13, par. 5-bis**, Law 196/2003 the information as per art. 13, paragraph 1, Law 196/2003 shall not be necessary in case CVs are received that are sent voluntarily by the relevant data subjects with a view to recruitment for job positions[8].

ii. **Do your country's laws require companies and entities doing business on the internet to inform consumers of the identity of who is collecting the data, if the provision of the requested data is voluntary or required and the steps taken by the data collector to ensure the confidentiality, the integrity and the quality of the data?**

Our law does not expressly requiere companies doing business on the Internet to inform consumers. Nevertheless, according to **art. 13, f),** D.lgs. 196/2003 all the data collectors (therefore also the companies doing business on the Internet) have to inform the consumers about the data controller and, where designated, the data controller's representative in the State's territory.

According to **art. 13, b)** D.lgs. 196/2003 all the data collectors have to inform about the obligatory or voluntary nature of providing the requested data.

Art. 32 (Obligations Applying to Providers of Publicly Available Electronic Communications Services) requires to the provider of a publicly available electronic communications service to take technical and organisational measures that are adequate in the light of the existing risk, in order to safeguard security of its services and ensure the confidentiality, integrity nd the quality of the personal data.

In case of a particular risk of a breach of network security, the provider of a publicly available electronic communications service shall inform contracting parties and, if possible, users concerning said risk and, when the risk lies outside the scope of the measures to be taken by said provider of all the possible remedies including an indication of the likely costs involved[9].

---

[7] Art. 13, par. 1, Dlgs. 196/2003: « *The data subject as well as any entity from whom or which personal data are collected shall be preliminarily informed, either orally or in writing, as to: a) the purposes and modalities of the processing for which the data are intended; b) the obligatory or voluntary nature of providing the requested data; c) the consequences if (s)he fails to reply; d) the entities or categories of entity to whom or which the data may be communicated, or who/which may get to know the data in their capacity as data processors or persons in charge of the processing, and the scope of dissemination of said data;* e) *the rights as per Section 7; f) the identification data concerning the data controller and, where designated, the data controller's representative in the State's territory pursuant to Section 5 and the data processor. If several data processors have been designated by the data controller, at least one among them shall be referred to and either the site on the communications network or the mechanisms for easily accessing the updated list of data processors shall be specified. If a data processor has been designated to provide responses to data subjects in case the rights as per Section 7 are exercised, such data processor shall be referred to* ».

[8] Art. 13, par. 5-bis, Law 196/2003: « *The information as per paragraph 1 shall not be necessary in case CVs are received that are sent voluntarily by the relevant data subjects with a view to recruitment for job positions. When first contacting a data subject that has sent his/her CV, the data controller shall be required to provide such data subject, also verbally, with a short information notice that shall include at least the items mentioned in paragraph 1, letters a., d., and f. . [Paragraph added by Section 6(2)a, item 2. of decree no. 70 dated 13 May 2011 as converted, with amendments, into Act no. 106 dated 12 July 2011]* ».

[9] Art. 32 Law 196/2003: « 1. *The provider of a publicly available electronic communications service shall take technical and organisational measures under the terms of Section 31 that are adequate in the light of the existing risk, in order to safeguard security of its services and with a view to taking the steps set forth in Section 32-bis hereof, also by way of other entities that have*

Art. 33 (Minimum Security Measures)[10] and **art. 34** (Processing by Electronic Means) of the Law 196/2003 specify the technical measures that the data subjetcs have to adopt in order to ensure the confidentiality, the integrity and the quality of the data [11].

iii. **Do your country's laws require websites to display a privacy policy and explain how personal information will be used before consumers enter the purchase process or any other transaction for which they must provide sensitive information?**

According to **Art. 13** Law 196/2003 requieres to all data collectors (therefore also the webpages' data collectors) explain how personal information will be used before consumers enter the purchase process.

iv. **Does the criminal law of your country penalize failing to provide the disclosures mentioned above (a.i; a.ii and a.iii)?**

No, it doesn't.

---

been tasked with delivering the said service.1-bis. Subject to compliance with the obligations set forth in Sections 30 and 31 hereof, any entity operating on electronic communications networks shall ensure that personal data may only be accessed by authorised personnel for legally authorised purposes. 1-ter. The measures referred to in paragraphs 1 and 1-bis above shall ensure the protection of traffic and location data and of any other personal data stored or transmitted against destruction, whether accidental or not, loss or alteration, whether accidental or not, and unauthorised or unlawful storage, processing, access or disclosure, and they shall also ensure implementation of a security policy. 2. Whenever security of service or personal data makes it necessary to also take measures applying to the network, the provider of a publicly available electronic communications service shall take those measures jointly with the provider of the public communications network. Failing an agreement between said providers, the dispute shall be settled, at the instance of either provider, by the Authority for Communications Safeguards in pursuance of the arrangements set out in the legislation in force. 3. In case of a particular risk of a breach of network security, the provider of a publicly available electronic communications service shall inform contracting parties and, if possible, users concerning said risk and, when the risk lies outside the scope of the measures to be taken by said provider pursuant to paragraphs 1, 1-bis and 2, of all the possible remedies including an indication of the likely costs involved. This information shall be also provided to the Garante and the Authority for Communications Safeguards ».

[10] Art. 33 Law 197/2003: « *1. Within the framework of the more general security requirements referred to in Section 31, or else provided for by specific regulations, data controllers shall be required in any case to adopt the minimum security measures pursuant either to this Chapter or to Section 58(3) in order to ensure a minimum level of personal data protection* ».

[11] Art. 34 Law 196/2003: « *measures referred to below are adopted in accordance with the arrangements laid down in the technical specifications as per Annex B: a) computerised authentication, b) implementation of authentication credentials management procedures, c) use of an authorisation system, d) regular update of the specifications concerning scope of the processing operations that may be performed by the individual entities in charge of managing and/or maintenancing electronic means, e) protection of electronic means and data against unlawful data processing operations, unauthorised access and specific software, f) implementation of procedures for safekeeping backup copies and restoring data and system availability,h) implementation of encryption techniques or identification codes for specific processing operations performed by health care bodies in respect of data disclosing health and sex life.1-ter. For the purpose of applying the provisions concerning the protection of personal data, a processing operation performed for administrative and accounting purposes shall by any processing operation that is related to the performance of organizational, administrative, financial and accounting activities irrespective of the nature of the processed data. The said purposes apply, in particular, to in-house organizational activities, the activities aimed at fulfilling contractual and precontractual obligations, managing employer-employee relationships, keeping accounting records, and implementing the legislation on taxation, trade unions, social security and welfare, and occupational health and safety. [Added by Section 6(2)a, item 5. of decree no. 70 dated 2011 as converted, with amendments, into Act no. 106 dated 12 July 2011]* ».

It represents only a breach of administrative rules.

The failing to provide the disclosures mentioned above is a breach of administrative rules according to **art. 161, 162-ter, D.lgs. 196/2003.**

Art. 161 Law 196/2003 criminalizes the data collector who does not provide or provides inadequate information to data subjects[12].

b. Act – illegal use and transfer/distribution?

i. **Does the criminal law of your country define the illegal transfer and distribution of private data?**

Yes.

Art. 4, l) and m), of the Law n. 196/2003 (D.lgs. 196/2003) defines the concepts of "communication" and "dissemination" of personal data[13].

Art. 167 of the Law 196/2003 criminalizes the unauthorized proccessing of personal data with a view to gain for himself or another or with intent to cause harm to another and that a harm is caused.

According to art. 4 Law 196/2003 **processing personal data** mean « *any operation, or set of operations, carried out with or without the help of electronic or automated means, concerning the collection, recording, organisation, keeping, interrogation, elaboration, modification, selection, retrieval, comparison, utilization, interconnection, blocking,* ***communication****,* ***dissemination****, erasure and destruction of data, whether the latter are contained or not in a data bank* ».

ii. **Does the criminal law of your country penalize the illegal use, transfer and/or distribution of private data?**

Yes.

Art. 167 (Unlawful Data Processing) of Law. 196/2003[14] criminalizes the unauthorized proccessing of personal data with a view to gain for himself or another or with intent to cause harm to another and that a harm is caused. According to art. 4 Law 196/2003 processing personal data mean « *any operation, or set of operations, carried out with or without the help of electronic or automated means, concerning the collection, recording, organisation, keeping, interrogation, elaboration, modification, selection, retrieval, comparison, utilization, interconnection,*

---

[12] Art. 161 Law 196/2003: « *1. Breach of the provisions referred to in Section 13 shall be punished by a fine consisting in payment of between six thousand and thirty-six thousand Euro. The amount may be increased by up to three times as much if it is found to be ineffective on account of the offender's economic status* ».

[13] Art. 4, l): « *'communication' shall mean disclosing personal data to one or more identified entities other than the data subject, the data controller's representative in the State's territory, the data processor and persons in charge of the processing in any form whatsoever, including by making available or interrogating such data* »; art. 4, m) Dlgs. 196/2003: « *'dissemination' shall mean disclosing personal data to unidentified entities, in any form whatsoever, including by making available or interrogating such data* ».

[14] Art. 167 Law 196/2003: « *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 ».*

blocking, communication, dissemination, erasure and destruction of data, whether the latter are contained or not in a data bank ».

c. Justification?

i. **Under which conditions does your country's law allow for the authorized collection, processing, transfer and distribution of private data?**

According to **art. 5, par 3,** Law 196/2003 (Subject-Matter and Scope of Application) shall not apply to processing of personal data carried out by a natural person for personal aims only, as long as the personal data ae not systematically communicated or disseminated to others[15].

According to **art. 11 Law 196/2003** every processing data have to respect the following rules: a) the personal data shall be processed lawfully and fairly; b) they have to be collected and recorded for specific, explicit and legitimate purpose s and used in further processing operations in a way that is not inconsistent with said purposes; c) the data have to be accurate and, when necessary, kept up to date; d) they have to be relevant, complete and not excessive in relation to the purposes for which they are collected or subsequently processed; e) they have to be kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data were collected or subsequently processed.

According to **art. 11, par, 2, Law 196/2003** any personal data that is processed in breach of the relevant provisions concerning the processing of personal data may not be used.

According to **art. 13** Law 196/2003 for an authorized collection, processing, transfer and distribution of private data the data collectors have to inform, either or ally or in writing the data subject as well as any entity from whom or which personal data are collected of the identity of who is collecting the data, if the provision of the requested data is voluntary or required and the steps taken by the data collector to ensure the confidentiality, the integrity and the quality of the data.

According to **art.18, par 2,** Law 196/2003 public bodies shall only be permitted to process personal data in order to discharge their institutional tasks. In processing the data, the public bodies shall abide by the prerequisites and limitations set out in this Code, by having also regard to the different features of the data, as well as in laws and regulations (art. 18, par 3).

According to **art.19 Law 196/2003** the public bodies may process data other than sensitive and judicial data also in the absence of laws or regulations providing expressly for such processing, subject to Section 18(2). To the public body to other public bodies is permitted to communicate personal data if it is envisaged by laws or regulations. Failing such laws or regulations, communication shall be permitted if it is necessary in order to discharge institutional tasks and may be started upon expiry of the term referred to in Section 39(2) if it has not been provided otherwise as specified therein.

The communication by a public body to private entities or profit-seeking public bodies as well as dissemination by a public body shall only be permitted if they are provided for by laws or regulations[16]

---

[15] Art. 5, par. 3, Law 196/2003: « *This Code shall only apply to the processing of personal data carried out by natural persons for exclusively personal purposes if the data are intended for systematic communication or dissemination. The provisions concerning liability and security referred to in Sections 15 and 31 shall apply in any case* ».

[16] Art. 15 Law 196/2003: « *1. Public bodies may process data other than sensitive and judicial data also in the absence of laws or*

According to **art. 23** Law 196/2003 in order to processing personal data private entities or profit-seeking public bodies shall only be allowed if the data subject gives his/her express consent. The consent hs to be given in writing if the processing concerns sensitve data[17] **Art. 24** Law 196/2003 establishes the cases in which the previous consent is not necessary for processing data[18]

---

regulations providing expressly for such processing, subject to Section 18(2). 2. Communication by a public body to other public bodies shall be permitted if it is envisaged by laws or regulations. Failing such laws or regulations, communication shall be permitted if it is necessary in order to discharge institutional tasks and may be started upon expiry of the term referred to in Section 39(2) if it has not been provided otherwise as specified therein. 3. Communication by a public body to private entities or profit-seeking public bodies as well as dissemination by a public body shall only be permitted if they are provided for by laws or regulations.3-bis. The information concerning performance of the tasks committed to any person that is in charge of public functions including the respective evaluation shall be made available by the public employer. Except where provided for by law, no information may be disclosed concerning nature of the medical conditions and/or personal or family circumstances resulting into a person's absence from the workplace or else the elements making up the evaluation or any information on the employment relationship between the aforementioned public employee and the public employer if they are suitable for disclosing any items of information referred to in section 4(1)d. Hereof »

[17] Art. 23 Law 196/2003: « *Processing of personal data by private entities or profit-seeking public bodies shall only be allowed if the data subject gives his/her express consent 2. The data subject's consent may refer either to the processing as a whole or to one or more of the operations thereof. 3. The data subject's consent shall only be deemed to be effective if it is given freely and specifically with regard to a clearly identified processing operation, if it is documented in writing, and if the data subject has been provided with the information referred to in Section 13. 4. Consent shall be given in writing if the processing concerns sensitive data* ».

[18] Art. 24 Law 196/2003: « *1. Consent shall not be required in the cases referred to in Part II as well as if the processing a) is necessary to comply with an obligation imposed by a law, regulations or Community legislation; b) is necessary for the performance of obligations resulting from a contract to which the data subject is a party, or else in order to comply with specific requests made by the data subject prior to entering into a contract; c) concerns data taken from public registers, lists, documents or records that are publicly available, without prejudice to the limitations and modalities laid down by laws, regulations and Community legislation with regard to their disclosure and publicity; d) concerns data relating to economic activities that are processed in compliance with the legislation in force as applying to business and industrial secrecy;e) is necessary to safeguard life or bodily integrity of a third party. If this purpose concerns the data subject and the latter cannot give his/her consent because (s)he is physically unable to do so, legally incapable or unable to distinguish right and wrong, the consent shall be given by the entity legally representing the data subject, or else by a next of kin, a family member, a person cohabiting with the data subject or, failing these, the manager of the institution where the data subject is hosted. Section 82(2) shall apply;f) is necessary for carrying out the investigations by defence counsel referred to in Act no. 397 of 07.12.2000, or else to establish or defend a legal claim, provided that the data are processed exclusively for said purposes and for no longer than is necessary therefor by complying with the legislation in force concerning business and industrial secrecy, dissemination of the data being ruled out; g) is necessary to pursue a legitimate interest of either the data controller or a third party recipient in the cases specified by the Garante on the basis of the principles set out under the law, unless said interest is overridden by the data subject's rights and fundamental freedoms, dignity or legitimate interests, dissemination of the data being ruled out; [Amended by Section 6(2)a, item 3. of decree no. 70 dated 13 May 2011 as converted, with amendments, into Act no. 106 dated 12 July 2011] h) except for external communication and dissemination, is carried out by no-profit associations, bodies or organisations, recognised or not, with regard either to entities having regular contacts with them or to members in order to achieve specific, lawful purposes as set out in the relevant memorandums, articles of association or collective agreements, whereby the mechanisms of utilisation are laid down expressly in a resolution that is notified to data subjects with the information notice provided for by Section 13,i) is necessary exclusively for scientific and statistical purposes in compliance with the respective codes of professional practice referred to in Annex A), or else*

ii. **What standard of need is required for an authorized collection and/or distribution (compelling, important, reasonable, convenient)?**

According to **art. 2** Law 196/2003 the data collectors in processing of personal data have to afford a high level of protection for the rights and freedoms in compliance with the principles of simplification, harmonisation and effectiveness of the mechanisms by which data subjects can exercise such rights and data controllers can fulf il the relevant obligations.

According to art. 3 Law. 196/2003 if the data processing is carried out through information systems and software they have to be configured by minimising the use of personal data and identification data, in such a way as to rule out their processing if the purposes sought in the individual cases can be achieved by using either anonymous data or suitablearrangements to allow identifying data subjects only in cases of necessity, respectively.

According to **art. 11** Law 196/2003 the data collector have to guarantee that the personal data have to be: a) processed lawfully and fairly; b) collected and recorded for specific, explicit and legitimate purposes and used in further processing operations in a way that is not inconsistent with said purposes; c) accurate and, when necessary, kept up to date; d) relevant, complete and not excessive in relation to the purposes for which they are collected or subsequently processed; e) kept in a form which permits identification of the data subject for no longer than is necessary for the purposes for which the data were collected or subsequently processed.

2. Violation of professional confidentiality

a. Object – type of private data?

i. Do your country's laws require that professionals disclose:

- Their information collection and management practices before collecting personal information from their patients or clients;

Yes.

According to **art. 13** Law 196/2003 all the data collectors (included the professionals processing data in the health care sector) before collecting personal data disclose to their patient or clients their collection and managment practices. Art. 77 law 196/2003 simplifies the arrangaments for data processing in the healt care sector[19].

---

exclusively for historical purposes in connection either with private archives that have been declared to be of considerable historical interest pursuant to Section 6(2) of legislative decree no. 499 of 29 October 1999, adopting the consolidated statute on cultural and environmental heritage, or with other private archives pursuant to the provisions made in the relevant codes; i-bis) concerns information contained in the CVs as per Section 13(5-bis); [Added by Section 6(2)a, item 3. of decree no. 70 dated 13 May 2011 as converted, with amendments, into Act no. 106 dated 12 July 2011] i-ter) except for dissemination and subject to Section 130 hereof, concerns communication of data between companies, bodies and/or associations and parent, subsidiary and/or related companies pursuant to Section 2359 of the Civil Code, or between the former and jointly controlled companies, or between consortiums, corporate networks and/or corporate joint ventures and the respective members, for the administrative and accounting purposes specified in Section 34(1-ter) hereof, providing such purposes are expressly referred to in a decision that shall be disclosed to data subjects jointly with the information notice referred to in Section 13 hereof. [Added by Section 6(2)a, item 3. of decree no. 70 dated 13 May 2011 as converted, with amendments, into Act no. 106 dated 12 July 2011] ».

[19] Art. 70 Law 196/2003: « *1. This Chapter shall lay down simplified arrangements that may be applied by the entities referred to in paragraph 2 a) to inform data subjects of the personal data collected either from them or from third parties, in pursuance of Section 13, paragraphs 1 and 4, b) to obtain data subjects' consent to the processing of personal data whenever this is required*

The professional of the health sector have to ensure that data subjects' rights, fundamental freedoms and dignity, as well as professional secrecy requirements are respected in organising the relevant services and discharging the relevant tasks, without prejudice to the provisions made in laws and regulations concerning arrangements to process sensitive data and minimum security measures (art.83 Law 196/2003).

- Their disclosure practices;

Yes, thet have also to disclosure their practices in processing data.

- Their professional ethical obligations;

No, it doesn't.

- And whether patients or clients have any control over the disclosure of their personal data?

Yes, they have to inform the patients or clients about thier rights over the disclosure of their data, as provided for **art. 13** Law 196/2003.

ii. Which data are specifically protected, if any?

Law 196/2003 guarantees a special protection to the identification, sensitive and judicial data.

iii. Does your country's penal law allow or even require clinicians, lawyers, priests, etc. to breach the confidentiality in certain situations or for certain reasons established by law? Under which standards would that be done? (e.g. reasonable cause to believe that there is abuse vs. seeing an abused child, women, elderly)?

Art. **200, par. 1,** of the Criminal Procedure Law guarantees the professional confidentiality for some subjects (i.e. Laywers, priets, clinicians, etc.)[20]. Nevertheless the Italian law can allow exceptionally breaching of the professional confidentiality (see for example art. 365 of Italian Penal Code, requiring to the medical personnel to inform the law enforcemente authorities if they discover during his work that a crime has been committed)[21].

---

under Section 76, c) to process personal data. 2. The simplified arrangements referred to in paragraph 1 shall be applicable a) by public health care bodies, b) by other private health care bodies and health care professionals, c) by the other public entities referred to in Section 80 ».

[20] Art. 200 c.p.p.: « *1. Non possono essere obbligati a deporre su quanto hanno conosciuto per ragione del proprio ministero, ufficio o professione, salvi i casi in cui hanno l'obbligo di riferirne all'autorità giudiziaria: a) i ministri di confessioni religiose, i cui statuti non contrastino con l'ordinamento giuridico italiano; b) gli avvocati, gli investigatori privati autorizzati, i consulenti tecnici e i notai; c) i medici e i chirurghi, i farmacisti, le ostetriche e ogni altro esercente una professione sanitaria; d) gli esercenti altri uffici o professioni ai quali la legge riconosce la facoltà di astenersi dal deporre determinata dal segreto professionale. 2. Il giudice, se ha motivo di dubitare che la dichiarazione resa da tali persone per esimersi dal deporre sia infondata, provvede agli accertamenti necessari. Se risulta infondata, ordina che il testimone deponga. 3. Le disposizioni previste dai commi 1 e 2 si applicano ai giornalisti professionisti iscritti nell'albo professionale, relativamente ai nomi delle persone dalle quali i medesimi hanno avuto notizie di carattere fiduciario nell'esercizio della loro professione. Tuttavia se le notizie sono indispensabili ai fini della prova del reato per cui si procede e la loro veridicità può essere accertata solo attraverso l'identificazione della fonte della notizia, il giudice ordina al giornalista di indicare la fonte delle sue informazioni ».*

[21] Art. 365: « *Chiunque, avendo nell'esercizio di una professione sanitaria prestato la propria assistenza od opera in casi che possono presentare i caratteri di un delitto pel quale si debba procedere d'ufficio, omette o ritarda di riferirne all'autorità indicata nell'articolo 361 è punito con la multa fino a euro 516. Questa disposizione non si applica quando il referto esporrebbe la persona assistita a procedimento penale* ».

According to our Penal Code the breaching of the confidentiality is allowed only for a right reason. **Art. 622, par.1, of** the Italian Penal Code criminalizes whoever discloses confidential information (secret) that he has known for his/her job, office or profession without a right reason or uses it for his profit or for the profit of another person. The perpetrator is punished, if the illegal act causes a damage, with the inprisonment up to 1 yeat and a fine from 30 to 516 euros[22].

b. Subject – Type of perpetrators?

Does the criminal law of your country identify the categories of professionals who are bound by specific confidentiality rules?

Yes, the criminal law (i.e. Arts. 361, 362 c.p.) mentions expressely the public funcionaries ("pubblici ufficiali") and the persons attended a need public service ("incaricato di servizio di pubblica necessità).

c. Act – illegal use and transfer/distribution?

Which acts (e.g. illegal collection, use, transfer and distribution) are specifically penalized by your country's criminal law?

Art. 167 Law 196/2003 criminalizes the illegal processing (including also the use, collection, transfer and distribution) of personal data with a view to gain for himself or another or with intent to cause harm to another.

3. Illegal processing of personal and private data

a. Object?

Does your criminal law penalize the illegal and unauthorized acquisition, processing, storage, analysis, manipulation, use, sale, transfer etc. of personal and private data?

Yes.

According to art. 167 Law 196/2003 the illegal processing of data can be criminalized if the the unauthorized proccessing of personal data is carried out with a view to gain for himself or another or with intent to cause harm to another and that a harm is caused.

According to art. 4 Law 196/2003 **processing personal data** mean « *any operation, or set of operations, carried out with or without the help of electronic or automated means, concerning the collection, recording, organisation, keeping, interrogation, elaboration, modification, selection, retrieval, comparison, utilization, interconnection, blocking, communication, dissemination, erasure and destruction of data, whether the latter are contained or not in a data bank* ».

b. Subject?

Does your criminal law identify specifically the categories of persons and entities included in this criminal prohibition and sanctions?

Yes.

The criminal law does not expressely identify the perpetrators ("whoever..."; "any person who..."). Nevertheless the

[22] Art. 622 c.p.: "*Chiunque, avendo notizia, per ragione del proprio stato o ufficio, o della propria professione o arte, di un segreto, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto può derivare nocumento, con la reclusione fino a un anno o con la multa da euro 30 a euro 516*".

perpetrators of these offences will be normally the "data controller" (any natural or legal person); the "data collector or processor" (any natural or legal person) and "any person in charge of the processing".

c. Act?

i. Does your criminal law penalize specific acts that constitute all or part of the illegal processing of personal and private data? Reply for each category listed below citing the relevant law and its provisions, if available:

Yes.

Our criminal law (Law 196/2003) criminalizes provides for an aggravating circunstance for specific acts of unauthorized proccessing of personal data. According to **art. 167, paragraph 1,** Law 196/2003 the **distribution** or **communication** of personal data or of personal data with a view to gain for himself or another or with intent to cause harm to another and that a harm is caused is punished with the inmprisonment from 1 to 3 years.

Art. 167,par. 2, Law 196/2003 provides for the same imprisonment if the unauthorized processing with a view to gain for himself or another or with intent to cause harm to another and that a harm is caused concerning operations carrying specific risks (art. 17 Law 196/2003), sensitive or judicial data (art. 20, art. 22, par. 8 and 11, art. 26, art. 27 Law 196/2003).

1. Illegal collection

2. Illegal use

3. Illegal retention

4. Illegal transfer

According to **art. 167** Law 196/2003 all these acts are criminalizez if they are carried out with a view to gain for himself or another or with intent to cause harm to another.

ii. Does it make a difference if these personal and private data are used, transferred etc. for police or law enforcement purposes?

Yes.

According to art. 25, par. 2, law 196/2003 the processing personal data,and expecially the communication and the dissemination of personal data for police purposes is allowed for purposes of defence or relating State security, or for the prevention,detection or suppression of offences.

4. Identity theft

(Note: identity theft occurs when someone appropriates another's personal information without his or her knowledge to commit theft or fraud. Identity theft is a vehicle for perpetrating fraud schemes. Typically, the victim is led to believe they are divulging sensitive personal information to a legitimate business or entity, sometimes as a response to an e-mail solicitation to update billing or membership information, or as an application for a fraudulent Internet job posting or loan.)

a. Object

i. Does your criminal law penalize identify theft? Please, cite the relevant law.

No, it doesn't, but it is possible to apply art. 494 p.c. (impersonation), if the structural elements of the criminal offences exist: specific intent (financial gain or damage); event (misleading in error the victim); conducts: attribution of a false name or quality.

ii. Does your criminal law proscribe specific forms of identity theft, like phishing, for example? Phishing is defined as a form of online identity theft that uses spoofed emails designed to lure recipients to fraudulent websites which attempt to trick them into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc.

No, it doesn't. There exists a large number of criminal provisions covering the "phenomenological phases" of the commission of the offences. The Italian legislation, in particular, is marked by a multiplicity of crimes that migh (ipothetically) be appliable[23]. But it doesn't exist an anti-phishing act or a specific criminal provision like in the U.S.A. (at State level).

b. Subject

Does your criminal law contain penal responsibility connected to a person's digital personality, or to his/her Avatar, or to his/her digital role in an internet based simulation game (e.g. Cityville, Farmville, etc.)? Please cite the relevant law.

No, it doesnt. The reference is to person (individual, physical) or to passwords and user names, which can identify a person online or using a computer system.

(c) Protection Against Illegal Content: ICT Related

1. Object

a. Child pornography - images of real or virtual children?

i. **Does your penal law criminalize the use of the internet for the purpose of storing, accessing, and disseminating child pornography? If so, please, cite the relevant law.**

Yes.

Art. 600-ter, par.1, of the Italian Penal Code criminalizes the distribution and dissemination also through the Internet of child pornography[24]. Art. 600-quater c.p. criminalizes also the procurement or possession of child pornography[25]

The mere access to child pornography is not criminalized.

ii. **In particular, does your criminal law:**

Create a new offense that targets criminals who use the Internet to lure and exploit children for sexual purposes?

Yes.

See below **art. 600-undecies** c.p. (child-grooming).

---

[23] For example: art. 615 ter, 615 quater, 640 ter, 640 (fraud); 648 bis (money laundering, for the financial manager who helps the phisher).

[24] Art. 600-quater c.p.: « *Chiunque, al di fuori delle ipotesi previste dall'articolo 600-ter, consapevolmente si procura o detiene materiale pornografico realizzato utilizzando minori degli anni diciotto, è punito con la reclusione fino a tre anni e con la multa non inferiore a euro 1.549. La pena è aumentata in misura non eccedente i due terzi ove il materiale detenuto sia di ingente quantità* ».

[25] Art. 600-quater.1 c.p.: « *Le disposizioni di cui agli articoli 600-ter e 600-quater si applicano anche quando il materiale pornografico rappresenta immagini virtuali realizzate utilizzando immagini di minori degli anni diciotto o parti di esse, ma la pena è diminuita di un terzo. Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali.*».

Make it a crime:

1. to transmit,

Yes.

Art. **600-ter, par. 3,** c.p. criminalizes whoever distributes and disseminates child pornography

make available,

Art. **600-ter, par. 3,** c.p. criminalizes whoever distributes, spreads and makes available child pornography

3. export

No.

The exportation of child pornography is not expressely punished.

4. and intentionally access child pornography on the Internet;

No, it doesn't. The illegal access to child pornography is not criminalized.

Allow judges to order the deletion of child pornography posted on computer systems in your country;

No, it is not expressly provided.

Allow a judge to order the forfeiture of any materials or equipment used in the commission of a child pornography offense;

Yes, the judge can order the "block" and the "removal" of illegal contents (such as child pornography).

See art. 600- septies c.p.[26]

For the jurisprudence of the Court of Cassation (see for example Cassazione penale , sez. III, sentenza 13.12.2004 n° 1481; Cass. Pen., Sez. V., 19.9.2011 (dep. 14.12.2011), n. 46504, Pres. Colonnese, Rel. Scalera) the judge can order the preventive forfeiture ("sequestro preventivo") of illegal contents (included also the child pornography) hold by the perpetrator, according to art. **600-septies c.p.** and **art. 321, paragraph 2, c.p.p.** (Italian Procedure penal Code), if there is the risk that disposition of the illegal material can aggravate or potract the consequenses of the crime or favour the commission of new crimes.

Criminalize:

1. Knowingly accessing child pornography on the internet

No, it doesn't.

[26] Art. 600-septies c.p.: « *Nel caso di condanna, o di applicazione della pena su richiesta delle parti a norma dell'articolo 444 del codice di procedura penale, per i delitti previsti dalla presente sezione, nonché dagli articoli 609-bis, quando il fatto è commesso in danno di un minore di anni diciotto o il reato è aggravato dalle circostanze di cui all'articolo 609-ter, primo comma, numeri 1), 5) e 5-bis), 609-quater, 609-quinquies, 609-octies, quando il fatto è commesso in danno di un minore di anni diciotto o il reato è aggravato dalle circostanze di cui all'articolo 609-ter, primo comma, numeri 1), 5) e 5-bis), e 609-undecies, è sempre ordinata, salvi i diritti della persona offesa alle restituzioni e al risarcimento dei danni, la confisca dei beni che costituiscono il prodotto, il profitto o il prezzo del reato. Ove essa non sia possibile, il giudice dispone la confisca di beni di valore equivalente a quelli che costituiscono il prodotto, il profitto o il prezzo del reato e di cui il condannato abbia, anche indirettamente o per interposta persona, la disponibilità. Si applica il terzo comma dell'articolo 322-ter* ».

2. Transmitting child pornography on the internet

Yes

Art. 600-ter, par. 3, of the Italian Penal Code criminalizes the distribution, diffusion and dissemination, also trough information systems, of child pornography[27].

3. Exporting child pornography on the internet

No.

Exporting child pornography is not expressely punished, but **art. 600-ter, par.3**, c.p. criminalizes the diffusion and dissemination through an information system.

4. Possessing child pornography on the internet for the purpose of, e.g., transmitting, exporting it…?

Yes.

The mere possession of real, simulated and virtual child pornography is punished (**art. 600-quater; 600-quater.1 c.p.**).

According to art.600-quater.1 c.p. the **virtual child pornography** concerning images realized with technics of graphic elaboration not associated totally or partially wit real situation and which quality make to appear as real situations that are not real[28].

For the offences concerning virtual child pornography the imprisonment is reduced to 1/3.

iii. Does your criminal law penalize the online solicitation of children for sexual purposes via social networking websites and chat rooms?

Yes.

The new **art.600-undecies**, c.p., introduced by Law n. 172 of the 1st October 2012 that ratifies the Lanzarote Convention, criminalizes the acts of child-grooming through the TIC's[29].

iv. Is the definition of child pornography in your criminal code close to that contained in international instruments (e.g. EU Directives)?

Yes.

The new definition of real child pornography (**art. 600-ter, par. 7, c.p.**), introduced by the Law n. 172/2012, is closed to the international instruments, and especially to the Lanzarote Convention of the Council of Europe and to the

---

[27] Art. 600-ter, par. 3, c.p.: « Chiunque, al di fuori delle ipotesi di cui al primo e al secondo comma, con qualsiasi mezzo, anche per via telematica, distribuisce, divulga, diffonde (2) o *pubblicizza il materiale pornografico di cui al primo comma, ovvero distribuisce o divulga notizie o informazioni finalizzate all'adescamento o allo sfruttamento sessuale di minori degli anni diciotto, è punito con la reclusione da uno a cinque anni e con la multa da euro 2.582 a euro* ».

[28] Art.600-quater.1 c.p.: "Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali".

[29] Art. 609-undecies (Adescamento di minorenni) « *chiunque, allo scopo di commettere i reati di cui agli articoli 600, 600-bis, 600-ter e 600-quater, anche se relativi al materiale pornografico di cui all'articolo 600-quater.1, 600-quinquies, 609-bis, 609-quater, 609-quinquies e 609-octies, adesca un minore di anni sedici, è punito, se il fatto non costituisce più grave reato, con la reclusione da uno a tre anni. Per adescamento si intende qualsiasi atto volto a carpire la fiducia del minore attraverso artifici, lusinghe o minacce posti in essere anche mediante l'utilizzo della rete internet o di altre reti o mezzi di comunicazione* ».

Directive 93/2011/UE[30].

v. Is secondary victimization avoided for victims of child pornography in your penal law?

Yes.

The minors victims of child pornography or prostitution offences are not criminalized by our criminal law.

According to the new **art. 352, comma 1-ter. c.p.p.,** introduced with the Law 172/2012, in the legal actions concerning child pornography offences if the the prosecutor ("pubblico ministero") has to gather information by a minor will be act with the help of a child psychologist or psychiatrist.

According to art. 392, paragraph 1-bis, of the Italian procedure penal Law, modified by Law 172/2012, in the legal actions concerning child pornography offences the prosecutor or the person under investigation can ask to gather evidence before a criminal trial ("*incidente probatorio*") with regard to the deposition of a minor.

In States where prostitution or the appearance in pornography is punishable under national criminal law, it should be possible not to prosecute or impose penalties under those laws where the child concerned has committed those acts as a result of being victim of sexual exploitation or where the child was compelled to participate in child pornography. Is this what your criminal law contemplates?

No, it doesn't.

vi. **Does your criminal law criminalize "virtual child" pornography? "Virtual child" pornography does not use real children or images of real identifiable children. When the image is not that of a real child, but a combination of millions of computer pixels crafted by an artist, can the government in your country ban this allegedly victimless creation? Please cite the applicable law and/or court decisions**.

Yes.

Art.600-quater.1 c.p. criminalizes the distribution, diffusion, procurement for himself and posession of virtual child pornography.

According to art. 600-quater.1 c.p. the **virtual child pornography** concerning images realized with technics of graphic elaboration totally or partially not associated with a real situation and which quality make to appear as real situations that are not real[31].

For the offences concerning virtual child pornography the imprisonment is reduced to 1/3.

See also the case law: **Tribunale Milano, 11th November 2010** (available at http://www.penale.it/page.asp?mode=1&IDPag=932).

[30] Art.600-ter, par.3, c.p.: « *Ai fini di cui al presente articolo per pornografia minorile si intende ogni rappresentazione, con qualunque mezzo, di un minore degli anni diciotto coinvolto in attività sessuali esplicite, reali o simulate, o qualunque rappresentazione degli organi sessuali di un minore di anni diciotto per scopi sessuali* ».

[31] Art.600-quater.1 c.p.: "Per immagini virtuali si intendono immagini realizzate con tecniche di elaborazione grafica non associate in tutto o in parte a situazioni reali, la cui qualità di rappresentazione fa apparire come vere situazioni non reali".

vii. Mens rea: To be liable, the person should both intend to enter a site where child pornography is available and know that such images can be found there. Penalties should not be applied to persons inadvertently accessing sites containing child pornography. Are these the requirements of your criminal law?

The Italian Penal Code does not criminalize the mere access to child pornography through the TIC's.

All child pornography offences provided for our Criminal Law requieres the perpetrator acts intentionally or willfully or with a special intent.

According to the new **art. 602-quater c.p.**, introduced into the Penal Code with the Law 172/2012, if the child pornography offences are committed against a minor of 18 years old the perpetrator can not excuse himself invoking the ignorance of the age of the victim, except for the cases of inevitable ignorance ("ignoranza inevitabile dell'età della persona offesa)[32].

b. Any other object where criminalization depends on the use of Information & Communication Technologies (ICT)

Does your criminal law penalize the following conducts? Please cite the relevant law.

1. creation and use of true anonymity sending and/or receiving material on the ICT?

No, it doesn't.

2. cyber-bullying?

No, it doesn't.

3. cyber-stalking?

No, it is not expressly criminalized. Nevertheless art. 612-bis c.p. ("atti persecutori") covers also the cases of cyber-stalking[33].

4. cyber-grooming?

Yes, the child grooming is expressly criminalized by **art. 600-undecies c.p.**

2. Act - creation/accession/possession/transfer/public distribution by ICT (give examples)

Cite specific laws that criminalize the creation (even if never used), the accession, the possession (even if only in private), the transfer, and the public distribution through the internet and other electronic means of materials beside

---

[32] Art. 602-quater (Ignoranza dell'eta' della persona offesa): "*Quando i delitti previsti dalla presente sezione sono commessi in danno di un minore degli anni diciotto, il colpevole non puo' invocare a propria scusa l'ignoranza dell'eta' dell a persona offesa, salvo che si tratti di ignoranza inevitabile*".

[33] Art. 612-bis c.p.: « *Salvo che il fatto costituisca più grave reato, è punito con la reclusione da sei mesi a quattro anni chiunque, con condotte reiterate, minaccia o molesta taluno in modo da cagionare un perdurante e grave stato di ansia o di paura ovvero da ingenerare un fondato timore per l'incolumita' propria o di un prossimo congiunto o di persona al medesimo legata da relazione affettiva ovvero da costringere lo stesso ad alterare le proprie abitudini di vita.*
La pena è aumentata se il fatto è commesso dal coniuge legalmente separato o divorziato o da persona che sia stata legata da relazione affettiva alla persona offesa. La pena è aumentata fino alla metà se il fatto è commesso a danno di un minore, di una donna in stato di gravidanza o di una persona con disabilità di cui all'articolo 3 della legge 5 febbraio 1992, n. 104, ovvero con armi o da persona travisata. Il delitto è punito a querela della persona offesa. Il termine per la proposizione della querela è di sei mesi. Si procede tuttavia d'ufficio se il fatto è commesso nei confronti di un minore o di una persona con disabilità di cui all'articolo 3 della legge 5 febbraio 1992, n. 104, nonchè quando il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio ».

those already mentioned above, specifically because of internet/electronic technology use.

Yes

Art. 600-ter, par 1, c.p. criminalizes the creation ("production") of child pornography[34].

Art. 600-ter, par 3, c.p. criminalizes the public distribution, dissemination thorugh the Internet

Art. 600-quater; art. 600-quater.1 c.p. criminalizes the possession of real and virtual child pornography

Art. 609-undecies c.p.: solicitation of children for sexual purposes committed also through the Internet and Information technologies.

(d) ICT Related Violations of Property, Including Intellectual Property

Does your criminal law specifically proscribe and penalize the following conducts perpetrated through the use of the ICT?

Please, cite the relevant law.

1. Fraud

Art. 640 ter p.c. (computer related fraud) criminalizes the alteration of a computer system and the intervention, without right, on data and information. Other structural objective elements are: damage and financial gain.

Art. 640 (fraud) criminalizes the "traditional fraud". But the criminal offence is applicable also, for example, when the phisher, deceiving an user, convinces him to provide user id and password to access to home banking system and to make a money transfer.

2. Infringement of Intellectual Property IP rights

L. n. 633/1941 provides many criminal offences related to criminal copyright infringement[35]. These offences could be divided in different categories: 1) provisions related to technological objects (software and data bases, art. 171 bis) or technological protection measures (art. 171 bis and art. 171 ter, lett. F-bis); 2) provisions related to "traditional works" and applicable also to phenomena or criminal activities committed in the cyberspace (for example the illegal distribution of works through websites, forum, social networks, art. 171 ter); 3) criminal offences which provide the conduct "upload a work in a network system/Internet" (art. 171, lett. A-bis and 171 ter, par. 2, lett. A-bis).

About Industrial Property, art. 473 pc criminalizes the abuse of trademarks or patent (use of counterfeit trademark or patent), which may be committed also in Internet, through websites, forum or social networks.

Art. 474 pc punishes also who "puts into circulation" products with counterfeit trademarks, which may be committed also through Internet.

3. Industrial espionage

Art. 621 pc criminalizes the disclosure of the content of secret documents

Art. 622 pc criminalizes the disclosure of bussiness and profesional secret

---

[34] Art. 600-ter, par. 1, c.p.: « *È punito con la reclusione da sei a dodici anni e con la multa da euro 24.000 a euro 240.000 chiunque: 1) utilizzando minori di anni diciotto, realizza esibizioni o spettacoli pornografici ovvero produce materiale pornografico* ».

[35] See, in particular, art. 171, 171 bis and 171 ter.

Art. 623 pc criminalizes the disclosure of scientific or industrial secrets.

These provisions are related to "common" or "traditional" crimes.

But art. 623 bis pc extends these "rules" to all types of communications, like Internet communications. Furthermore the disclosure may be carried out by any type of means (included technological means).

(e) Criminalization of Acts Committed in the Virtual World

Does your criminal law penalize the commission of crimes committed in the virtual world like, for example, virtual child pornography, virtual violence, virtual graffiti, cyber-defamation, sexual harassment, harassment at work, without any involvement of real persons, only virtual representation? Please cite the relevant law and provide details.

(f) Non-Compliance Offenses

Does you criminal law penalize non cooperation with law enforcement agencies in the field of cybercrime?

No, it doesn't, but after the implementation of the Cybercrime Convention (L. 48/2008) cooperation with LEAs is encouraged

Duties to cooperate can be duties to retain and store information, to produce/deliver information as required by a production order, to give access to cyber systems to install filters or devices, etc. Is the breach of the duty to cooperate also enforced through administrative sanctions? Cite the relevant law and provide details.

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

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 defence counsel, the person under investigation, the injured party, or any other private party. Defence 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 specialising 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 fulfil 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.

Art. 132-bis *(Procedures Established by Providers)* **provides:** 1. Providers shall establish internal procedures to meet the requests made in compliance with the provisions that envisage access to users' personal data.

2. Upon demand, providers shall provide the Garante, having regard to the respective scope of competence, with information on the procedures referred to in paragraph 1, the number of requests received, the legal justification invoked and their response.

About administrative sanctions, **Art. 162-bis** *(Penalties Applying to Traffic Data Retention)* **provides:** 1. Any violation of the provisions set forth in section 132(1) and (1-bis) shall be punished by an administrative fine ranging from Euro 10,000 to 50,000, unless the facts at issue are established as a criminal offence and without prejudice to section 5(2) of the legislative decree transposing directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006

(D) Complementary optional information concerning law and practice (including statistics)

(1) Are cybercrimes included as such in the collection of data on crime in your country?

There aren't official statistics about cybercrime.

(2) Is there in your country a website that provides data and information on the occurrence, seriousness, cost, impact etc. of cyber-crimes in your country? If "yes", provide the website electronic address.

No, there isn't

(3) Do victimization surveys in your country include questions on cyber-crimes?

No.

(4) What types of computer crime / computer fraud are most often reported in your country?

It is difficult to collect data and information about computer crime and computer fraud. Some associations provide statistics for specific sectors, for example on phishing (http://www.anti-phishing.it/)

(5) Do law enforcement and prosecution in your country have a computer crimes unit? If so, how many officers/prosecutors are in it?

In each district of the Court of Appeal there is an unit of public prosecutors, but in Milan it is possible to find the unit most organized. About police, Guardia di Finanza, Carabinieri and Poliza have specific units. Polizia delle telecomunicazioni has specific competence in the fight against child-pornography (also in Internet)

(6) Does your or any law school in the country offer courses on cyber-crime? Please provide a website address.

Yes. At the Legal Science Department of the University of Verona there is a specific course on cybercrime (prof. Lorenzo Picotti, please visit http://www.giurisprudenza.univr.it/fol/main?ent=persona&id=662&lang=it). There is also one course by the University of Milano – Bicocca.

(7) Is the subject of cybercrime included in the training and/or continuing education of judges, prosecutors and police?

Consiglio Superiore della Magistratura organizes courses also on cybercrime, inviting also external experts. Recently, by the cybercrime unit of the Tribunal of Milan, the public prosecutors, in partnership with universities (like University of Verona and the group coordinated by prof. Picotti) have implemented an e-learning platforms (reference: Francesco Cajani).

(8) Please identify whether the following forms and means of cybercrime (1) occur frequently, (2) occur infrequently, or (3) have not occurred in your country, by placing an "X" as appropriate in the following table:

In Italy there are not official statistics and there are structural problems in collecting data (for example because of fear of negative publicity for companies that have suffered cyber attacks and data theft).