

**Cybercrime legislation – country profile**

**ITALY**

*This profile has been prepared within the framework of the Council of Europe’s capacity building projects on cybercrime in view of sharing information and assessing the current state of implementation of the Convention on Cybercrime under domestic legislation. It does not necessarily reflect official positions of the country covered or of the Council of Europe.*

Comments may be sent to:

Economic Crime Division  
 Directorate General of Human Rights and Legal Affairs  
 Council of Europe, Strasbourg, France

Tel: +33-3-9021-4506  
 Fax: +33-3-9021-5650  
 Email: [alexander.seger@coe.int](mailto:alexander.seger@coe.int)  
[www.coe.int/cybercrime](http://www.coe.int/cybercrime)

<b>Country:</b>	<b>Italy</b>
Signature of Convention:	23 November 2001
Ratification/accession:	5 April 2008
<b>Provisions of the Convention</b>	<b>Corresponding provisions/solutions in national legislation</b> <i>(pls quote or summarise briefly; pls attach relevant extracts as an appendix)</i>
<b>Chapter I – Use of terms</b>	
<b>Article 1 – “Computer system”, “computer data”, “service provider”, “traffic data”:</b> For the purposes of this Convention: a “computer system” means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs	<b>Art. 1 CoC is partially implemented.</b>  The Italian Criminal Code (“Codice penale”) does not define all the terms of art. 1 CoC.

<p>automatic processing of data;</p> <p>b "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;</p> <p>c "service provider" means:</p> <p>i any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and</p> <p>ii any other entity that processes or stores computer data on behalf of such communication service or users of such service;</p> <p>d "traffic data" means any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service</p>	<p>A definition of the term "computer document" is provided in art 1, lett. p) of Law n. 82/2005 ("Digital Administration Code").</p> <p>A definition of the term "traffic data" is provided in art. 4, lett. h) D.lgs. n. 196/2003 (Data Protection Act), but it is more restricted than art. 1, lett. d) CoC.</p>
<p><b>Chapter II – Measures to be taken at the national level</b>  <b>Section 1 – Substantive criminal law</b></p>	
<p><i>Title 1 – Offences against the confidentiality, integrity and availability of computer data and systems</i></p>	
<p><b>Article 2 – Illegal access</b>  Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p><b>Partially covered by art. 615ter c.p.</b>  Art. 615ter c.p. criminalizes only the access to an information or telecommunication system protected by security measures, without requiring the infringement of them.</p> <p>The provision criminalizes also the unauthorized "permanence" in such system.</p> <p>Art. 615ter c.p. does not define the term "security measures".</p> <p><b>Art. 615-ter. Accesso abusivo ad un sistema informatico o telematico.</b>  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.</p> <p>La pena è della reclusione da uno a cinque anni:</p> <p>1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al</p>

	<p>servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;</p> <p>2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;</p> <p>3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.</p> <p>Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici o telematici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.</p> <p>Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.</p>
<p><b>Article 3 – Illegal interception</b>  Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.</p>	<p><b>Covered by art. 617<sup>quater</sup>, 617<sup>quinquies</sup>, 617<sup>sexies</sup> c.p and art. 623<sup>bis</sup> c.p.</b>  The provisions apply to all kind of communications, without distinction between public or non-public transmissions as required by art. 3 CoC.</p> <p>The interception of “electromagnetic emissions” could be covered by art. 623<sup>bis</sup> c.p.</p> <p>Art. 617<sup>quater</sup>, 617<sup>sexies</sup> c.p. do not require expressly that the illegal interception must be committed by using technical devices, as required by art. 3 CoC.</p> <p>Art. 617<sup>quinquies</sup> c.p. criminalizes the installation of devices adapted to intercept, obstruct or interrupt communications between information systems.</p>
<p><b>Article 4 – Data interference</b>  1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or</p>	<p><b>Covered by art. 635<sup>bis</sup> c.p.</b>  Art. 635<sup>ter</sup> c.p. criminalizes the interference concerning computer data used by the State, or other public body or computer data that have however a public</p>

<p>suppression of computer data without right. 2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.</p>	<p>utility.</p> <p>Both of the provisions refer the interference not only to computer data, but also to information and programs.</p> <p>The legislator did not take into consideration the possibility to criminalise only conducts causing serious harm, as provided for art. 4, para 2, CoC.</p>
<p><b>Article 5 – System interference</b> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data</p>	<p><b>Covered by art. 635quater c.p.</b> Art. 635<i>quinquies</i> c.p. criminalizes the interference concerning information and telecommunication systems that have a public utility. <b>Art. 635-quater. Danneggiamento di sistemi informatici o telematici</b>Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-<i>bis</i>, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni. Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.</p> <p><b>Spam could be criminalize by art. 167 (illegal treatment of personal data) D.lgs. 196/2003 (Data Protection Act).</b></p>
<p><b>Article 6 – Misuse of devices</b> 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right: a the production, sale, procurement for use, import, distribution or otherwise making available of:  i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5; ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed,</p>	<p><b>Covered by art. 615quater, quinquies c.p.</b> Art. 615<i>quater</i> c.p. criminalizes the illegal detention and diffusion of access codes to information or telecommunication systems. Art. 615<i>quinquies</i> c.p. criminalizes the diffusion of equipment, device or programs directed to damage or interrupt the functioning of an information or telecommunication system.</p> <p><b>Art. 615-quater. Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici.</b></p>

<p>with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and</p> <p>b the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.</p> <p>2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.</p> <p>3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.</p>	<p>Chiunque, al fine di procurare a sé o ad altri un profitto o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce indicazioni o istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a euro 5.164.</p> <p>La pena è della reclusione da uno a due anni e della multa da euro 5.164 a euro 10.329 se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.</p>
<p><i>Title 2 – Computer-related offences</i></p>	
<p><b>Article 7 – Computer-related forgery</b></p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.</p>	<p><b>See by art. 491bis c.p.</b>  <b>Art. 491-bis. Documenti informatici.</b>          Se 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.”</p>
<p><b>Article 8 – Computer-related fraud</b></p> <p>Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:</p>	<p><b>See section 640ter c.p.</b></p> <p>Art. 640ter c.p. requires that the subject gains for himself or another person an illegal profit causing an harm to another.</p>

<p>a any input, alteration, deletion or suppression of computer data;</p> <p>b any interference with the functioning of a computer system,</p> <p>with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.</p>	<p><b>Art. 640-ter.Frode informatica.</b>          Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o ad esso pertinenti, procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 51 a euro 1.032.</p> <p>La pena è della reclusione da uno a cinque anni e della multa da euro 309 a euro 1.549 se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema.</p> <p>Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante.</p>
<p><i>Title 3 – Content-related offences</i></p>	
<p><b>Article 9 – Offences related to child pornography</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:</p> <p>a producing child pornography for the purpose of its distribution through a computer system;</p> <p>b offering or making available child pornography through a computer system;</p> <p>c distributing or transmitting child pornography through a computer system;</p> <p>d procuring child pornography through a computer system for oneself or for another person;</p> <p>e possessing child pornography in a computer system or on a computer-data storage medium.</p> <p>2 For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:</p> <p>a a minor engaged in sexually explicit conduct;</p> <p>b a person appearing to be a minor engaged in sexually explicit conduct;</p>	<p><b>Covered by art. 600ter, quarter, quarter.1, quinquies, sexies, septies c.p.</b></p> <p>Art. 600ter c.p. defines a “minor” as a person under 18 years old.</p> <p>Art. 600quarter.1, paragraph 2, c.p. defines the concept of “virtual pornography”</p> <p>Art. 600quarter c.p. criminalizes the possession of child pornography.</p> <p>Art. 600quinquies c.p. criminalizes the organization of tourist rates with the aim to exploit the child pornography. The provision is not relevant.</p> <p>Art. 600sexies c.p. provides for some aggravating circumstances.</p> <p>Art. 600septies c.p. provides for the sanctions of confiscation and other additional sanctions.</p>

<p>c realistic images representing a minor engaged in sexually explicit conduct</p> <p>3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.</p> <p>4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.</p>	
<p><i>Title 4 – Offences related to infringements of copyright and related rights</i></p>	
<p><b>Article 10 – Offences related to infringements of copyright and related rights</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.</p> <p>3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.</p>	<p><b>Covered by art. 171a-bis, 171bis, 171ter, 171 octies, 174ter of Italian Copyright Act (Law n. 633/1941).</b></p> <p><b>Art. 171-bis</b></p> <p>1. Chiunque abusivamente duplica, per trarne profitto, programmi per elaboratore o ai medesimi fini importa, distribuisce, vende, detiene a scopo commerciale o imprenditoriale o concede in locazione programmi contenuti in supporti non contrassegnati dalla Società italiana degli autori ed editori (SIAE), è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La stessa pena si applica se il fatto concerne qualsiasi mezzo inteso unicamente a consentire o facilitare la rimozione arbitraria o l'elusione funzionale di dispositivi applicati a protezione di un programma per elaboratori. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.</p> <p>2. Chiunque, al fine di trarne profitto, su supporti non contrassegnati SIAE riproduce, trasferisce su altro supporto, distribuisce, comunica, presenta o dimostra in pubblico il contenuto di una banca di dati in violazione delle disposizioni di cui agli articoli 64-quinquies e 64-sexies, ovvero esegue l'estrazione o il reimpiego della banca di dati in violazione delle disposizioni di cui agli articoli 102-bis e 102-ter, ovvero distribuisce, vende o concede in locazione una banca di dati, è soggetto alla pena della reclusione da sei mesi a tre anni e della multa da euro 2.582 a euro 15.493. La pena non è inferiore nel minimo a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.</p> <p><b>Art. 171-ter</b></p> <p>1. È punito, se il fatto è commesso per uso non personale, con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 15.493 chiunque a fini di</p>

	<p>lucro:</p> <p>a) abusivamente duplica, riproduce, trasmette o diffonde in pubblico con qualsiasi procedimento, in tutto o in parte, un'opera dell'ingegno destinata al circuito televisivo, cinematografico, della vendita o del noleggio, dischi, nastri o supporti analoghi ovvero ogni altro supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive assimilate o sequenze di immagini in movimento;</p> <p>b) abusivamente riproduce, trasmette o diffonde in pubblico, con qualsiasi procedimento, opere o parti di opere letterarie, drammatiche, scientifiche o didattiche, musicali o drammatico-musicali, ovvero multimediali, anche se inserite in opere collettive o composite o banche dati;</p> <p>c) pur non avendo concorso alla duplicazione o riproduzione, introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, o distribuisce, pone in commercio, concede in noleggio o comunque cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della televisione con qualsiasi procedimento, trasmette a mezzo della radio, fa ascoltare in pubblico le duplicazioni o riproduzioni abusive di cui alle lettere a) e b);</p> <p>d) detiene per la vendita o la distribuzione, pone in commercio, vende, noleggia, cede a qualsiasi titolo, proietta in pubblico, trasmette a mezzo della radio o della televisione con qualsiasi procedimento, videocassette, musicassette, qualsiasi supporto contenente fonogrammi o videogrammi di opere musicali, cinematografiche o audiovisive o sequenze di immagini in movimento, od altro supporto per il quale è prescritta, ai sensi della presente legge, l'apposizione di contrassegno da parte della Società italiana degli autori ed editori (S.I.A.E.), privi del contrassegno medesimo o dotati di contrassegno contraffatto o alterato;</p> <p>e) in assenza di accordo con il legittimo distributore, ritrasmette o diffonde con qualsiasi mezzo un servizio criptato ricevuto per mezzo di apparati o parti di apparati atti alla decodificazione di trasmissioni ad accesso condizionato;</p> <p>f) introduce nel territorio dello Stato, detiene per la vendita o la distribuzione, distribuisce, vende, concede in noleggio, cede a qualsiasi titolo, promuove commercialmente, installa dispositivi o elementi di decodificazione speciale che consentono l'accesso ad un servizio criptato senza il pagamento del canone dovuto.</p> <p>f-bis) fabbrica, importa, distribuisce, vende, noleggia, cede a qualsiasi titolo, pubblicizza per la vendita o il noleggio, o detiene per scopi commerciali, attrezzature, prodotti o componenti ovvero presta servizi che abbiano la prevalente finalità o l'uso commerciale di eludere efficaci misure tecnologiche di</p>
--	---



cui all'art. 102-quater ovvero siano principalmente progettati, prodotti, adattati o realizzati con la finalità di rendere possibile o facilitare l'elusione di predette misure. Fra le misure tecnologiche sono comprese quelle applicate, o che residuano, a seguito della rimozione delle misure medesime conseguentemente a iniziativa volontaria dei titolari dei diritti o ad accordi tra questi ultimi e i beneficiari di eccezioni, ovvero a seguito di esecuzione di provvedimenti dell'autorità amministrativa o giurisdizionale;

h) abusivamente rimuove o altera le informazioni elettroniche di cui all'articolo 102 quinquies, ovvero distribuisce, importa a fini di distribuzione, diffonde per radio o per televisione, comunica o mette a disposizione del pubblico opere o altri materiali protetti dai quali siano state rimosse o alterate le informazioni elettroniche stesse.

2. È punito con la reclusione da uno a quattro anni e con la multa da euro 2.582 a euro 15.493 chiunque:

a) riproduce, duplica, trasmette o diffonde abusivamente, vende o pone altrimenti in commercio, cede a qualsiasi titolo o importa abusivamente oltre cinquanta copie o esemplari di opere tutelate dal diritto d'autore e da diritti connessi;

*a-bis) in violazione dell'art. 16, a fini di lucro, comunica al pubblico immettendola in un sistema di reti telematiche, mediante connessioni di qualsiasi genere, un'opera dell'ingegno protetta dal diritto d'autore, o parte di essa;*

b) esercitando in forma imprenditoriale attività di riproduzione, distribuzione, vendita o commercializzazione, importazione di opere tutelate dal diritto d'autore e da diritti connessi, si rende colpevole dei fatti previsti dal comma 1;

c) promuove o organizza le attività illecite di cui al comma 1.

3. La pena è diminuita se il fatto è di particolare tenuità.

4. La condanna per uno dei reati previsti nel comma 1 comporta:

a) l'applicazione delle pene accessorie di cui agli articoli 30 e 32-bis del codice penale;

b) la pubblicazione della sentenza in uno o più quotidiani, di cui almeno uno a diffusione nazionale, e in uno o più periodici specializzati;

c) la sospensione per un periodo di un anno della concessione o autorizzazione di diffusione radiotelevisiva per l'esercizio dell'attività produttiva o commerciale.

5. Gli importi derivanti dall'applicazione delle sanzioni pecuniarie previste dai precedenti commi sono versati all'Ente nazionale di previdenza ed assistenza per i pittori e scultori, musicisti, scrittori ed autori drammatici.

**Art. 171-octies**

1. Qualora il fatto non costituisca più grave reato, è punito con la reclusione da sei mesi a tre anni e con la multa da euro 2.582 a euro 25.822 chiunque a fini fraudolenti produce, pone in vendita, importa, promuove, installa, modifica, utilizza per uso pubblico e privato apparati o parti di apparati atti alla decodificazione di trasmissioni audiovisive ad accesso condizionato effettuate via etere, via satellite, via cavo, in forma sia analogica sia digitale. Si intendono ad accesso condizionato tutti i segnali audiovisivi trasmessi da emittenti italiane o estere in forma tale da rendere gli stessi . visibili esclusivamente a gruppi chiusi di utenti selezionati dal soggetto che effettua l'emissione del segnale, indipendentemente dalla imposizione di un canone per la fruizione di tale servizio.

2. La pena non è inferiore a due anni di reclusione e la multa a euro 15.493 se il fatto è di rilevante gravità.

**Art. 171-octies-1**

1. Chiunque si rifiuti senza giustificato motivo di rispondere alle domande del giudice ai sensi dell'articolo 156-ter ovvero fornisce allo stesso false informazioni è punito con le pene previste dall'articolo 372 del codice penale, ridotte della metà.

**Art. 171-nonies**

1. La pena principale per i reati di cui agli articoli 171-bis, 171-ter e 171-quater è diminuita da un terzo alla metà e non si applicano le pene accessorie a colui che, prima che la violazione gli sia stata specificatamente contestata in un atto dell'autorità giudiziaria, la denuncia spontaneamente o, fornendo tutte le informazioni in suo possesso, consente l'individuazione del promotore o organizzatore dell'attività illecita di cui agli articoli 171-ter e 171-quater, di altro duplicatore o di altro distributore, ovvero il sequestro di notevoli quantità di supporti audiovisivi e fonografici o di strumenti o materiali serviti o destinati alla commissione dei reati.

2. Le disposizioni del presente articolo non si applicano al promotore o organizzatore delle attività illecite previste dall'articolo 171-bis, comma 1, e dall'articolo 171-ter, comma 1.

**Art. 1-4 Law n. 633/1941 define the term protected works.**

The provisions do not require expressly that the illegal acts must be committed through a computer system.

*Title 5 – Ancillary liability and sanctions*

**Article 11 – Attempt and aiding or abetting**

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, an attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, and 9.1.a and c. of this Convention.

3 Each Party may reserve the right not to apply, in whole or in part, paragraph 2 of this article.

**Attempt is covered by art. 56 c.p.**

**Art. 56. Delitto tentato.**

Chi compie atti idonei, diretti in modo non equivoco a commettere un delitto, risponde di delitto tentato, se l'azione non si compie o l'evento non si verifica. Il colpevole di delitto tentato è punito:; con la reclusione non inferiore a dodici anni, se la pena stabilita è l'ergastolo; e, negli altri casi con la pena stabilita per il delitto, diminuita da un terzo a due terzi.

Se il colpevole volontariamente desiste dall'azione, soggiace soltanto alla pena per gli atti compiuti, qualora questi costituiscano per sé un reato diverso.

Se volontariamente impedisce l'evento, soggiace alla pena stabilita per il delitto tentato, diminuita da un terzo alla metà.

**Aiding and abetting are covered by art. 110 c.p.**

**Art. 110. Pena per coloro che concorrono nel reato.**

Quando più persone concorrono nel medesimo reato, ciascuna di esse soggiace alla pena per questo stabilita, salve le disposizioni degli articoli seguenti

**Article 12 – Corporate liability**

1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for a criminal offence established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within it, based on:

- a a power of representation of the legal person;
- b an authority to take decisions on behalf of the legal person;
- c an authority to exercise control within the legal person.

2 In addition to the cases already provided for in paragraph 1 of this article, each Party shall take the measures necessary to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of a criminal offence established in accordance with this Convention for the benefit of that legal person by a natural person acting under its authority.

3 Subject to the legal principles of the Party, the liability of a legal person may be criminal, civil or administrative.

4 Such liability shall be without prejudice to the criminal liability of the natural persons who have committed the offence.

**Covered by art. 24, 24bis, 25 quinquies D.lgs. 231/2001 (Responsabilità amministrativa da reato).**

**Article 13 – Sanctions and measures**

**Article 13 (1) is covered by the above-mentioned articles (art. 491bis,**

<p>1 Each Party shall adopt such legislative and other measures as may be necessary to ensure that the criminal offences established in accordance with Articles 2 through 11 are punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty.</p> <p>2 Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions or measures, including monetary sanctions.</p>	<p>art. 615<i>ter</i>, <i>quater</i>, <i>quinquies</i>, art. 635<i>bis</i>, <i>ter</i>, <i>quater</i>, <i>quinquies</i>, 617<i>quater</i>, <i>quinquies</i>, <i>sexies</i>, art. 623<i>bis</i> c.p., art. 600<i>ter</i>, <i>quater</i>, <i>quater.1</i>, <i>quinquies</i>, <i>sexies</i>, <i>septies</i> c.p.; art. 171a-bis, 171<i>bis</i>, <i>ter</i>, <i>octies</i>, art. 174<i>ter</i> Law n. 633/1941).</p> <p><b>Article 13 (2) is covered by art. 24, 24<i>bis</i>, 25<i>quinquies</i> D.lgs 231/2003.</b></p> <p>See also general provisions of Criminal Code (art. 17 ss. c.p.)</p>
<p><b>Section 2 – Procedural law</b></p>	
<p><b>Article 14 – Scope of procedural provisions</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish the powers and procedures provided for in this section for the purpose of specific criminal investigations or proceedings.</p> <p>2 Except as specifically provided otherwise in Article 21, each Party shall apply the powers and procedures referred to in paragraph 1 of this article to:</p> <ul style="list-style-type: none"> <li>a the criminal offences established in accordance with Articles 2 through 11 of this Convention;</li> <li>b other criminal offences committed by means of a computer system; and</li> <li>c the collection of evidence in electronic form of a criminal offence.</li> </ul> <p>3 a Each Party may reserve the right to apply the measures referred to in Article 20 only to offences or categories of offences specified in the reservation, provided that the range of such offences or categories of offences is not more restricted than the range of offences to which it applies the measures referred to in Article 21. Each Party shall consider restricting such a reservation to enable the broadest application of the measure referred to in Article 20.</p> <p>b Where a Party, due to limitations in its legislation in force at the time of the adoption of the present Convention, is not able to apply the measures referred to in Articles 20 and 21 to communications being transmitted within a computer system of a service provider, which system:</p> <ul style="list-style-type: none"> <li>i is being operated for the benefit of a closed group of users, and</li> <li>ii does not employ public communications networks and is</li> </ul>	<p><b>See below (Articles 16-21).</b></p>

<p>not connected with another computer system, whether public or private, that Party may reserve the right not to apply these measures to such communications. Each Party shall consider restricting such a reservation to enable the broadest application of the measures referred to in Articles 20 and 21</p>	
<p><b>Article 15 – Conditions and safeguards</b> 1 Each Party shall ensure that the establishment, implementation and application of the powers and procedures provided for in this Section are subject to conditions and safeguards provided for under its domestic law, which shall provide for the adequate protection of human rights and liberties, including rights arising pursuant to obligations it has undertaken under the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms, the 1966 United Nations International Covenant on Civil and Political Rights, and other applicable international human rights instruments, and which shall incorporate the principle of proportionality. 2 Such conditions and safeguards shall, as appropriate in view of the nature of the procedure or power concerned, <i>inter alia</i>, include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure. 3 To the extent that it is consistent with the public interest, in particular the sound administration of justice, each Party shall consider the impact of the powers and procedures in this section upon the rights, responsibilities and legitimate interests of third parties.</p>	<p><b>See below (Articles 16-21).</b></p>
<p><b>Article 16 – Expedited preservation of stored computer data</b> 1 Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification. 2 Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored computer data in the person's possession or control, the Party shall adopt such legislative and other measures as may</p>	<p><b>Covered by art. 132, paragraph 4ter and 4quater D. Lgs. 196/2003 (Data Protection Act)</b> <b>Art. 132. Conservazione di dati di traffico per altre finalità</b> 4-ter. Il Ministro dell'interno o, su sua delega, i responsabili degli uffici centrali specialistici in materia informatica o telematica della Polizia di Stato, dell'Arma dei carabinieri e del Corpo della guardia di finanza, nonché gli altri soggetti indicati nel comma 1 dell'articolo 226 delle norme di attuazione, di coordinamento e transitorie del codice di procedura penale, di cui al decreto legislativo 28 luglio 1989, n. 271, possono ordinare, anche in relazione alle eventuali richieste avanzate da autorità investigative straniere, ai fornitori e agli</p>

<p>be necessary to oblige that person to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure. A Party may provide for such an order to be subsequently renewed.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige the custodian or other person who is to preserve the computer data to keep confidential the undertaking of such procedures for the period of time provided for by its domestic law.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p>operatori di servizi informatici o telematici di conservare e proteggere, secondo le modalità indicate e per un periodo non superiore a novanta giorni, i dati relativi al traffico telematico, esclusi comunque i contenuti delle comunicazioni, ai fini dello svolgimento delle investigazioni preventive previste dal citato articolo 226 delle norme di cui al decreto legislativo n. 271 del 1989, ovvero per finalità di accertamento e repressione di specifici reati. Il provvedimento, prorogabile, per motivate esigenze, per una durata complessiva non superiore a sei mesi, può prevedere particolari modalità di custodia dei dati e l'eventuale indisponibilità dei dati stessi da parte dei fornitori e degli operatori di servizi informatici o telematici ovvero di terzi.</p>
<p><b>Article 17 – Expedited preservation and partial disclosure of traffic data</b></p> <p>1 Each Party shall adopt, in respect of traffic data that is to be preserved under Article 16, such legislative and other measures as may be necessary to:</p> <p>a ensure that such expeditious preservation of traffic data is available regardless of whether one or more service providers were involved in the transmission of that communication; and</p> <p>b ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a sufficient amount of traffic data to enable the Party to identify the service providers and the path through which the communication was transmitted.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p><b>Covered in part by art. 244, paragraph 2, c.p.p.</b></p> <p><b>Art. 244. Casi e forme delle ispezioni.</b></p> <p>2. Se il reato non ha lasciato tracce o effetti materiali, o se questi sono scomparsi o sono stati cancellati o dispersi, alterati o rimossi, l'autorità giudiziaria descrive lo stato attuale e, in quanto possibile, verifica quello preesistente, curando anche di individuare modo, tempo e cause delle eventuali modificazioni. L'autorità giudiziaria può disporre rilievi segnaletici, descrittivi e fotografici e ogni altra operazione tecnica, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione.</p>
<p><b>Article 18 – Production order</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order:</p> <p>a a person in its territory to submit specified computer data in that person's possession or control, which is stored in a computer system or a computer-data storage medium; and</p> <p>b a service provider offering its services in the territory of the Party to submit subscriber information relating to such services in that service</p>	<p><b>Article 18 (1) lit. a is covered in part by art. 256, paragraph 1, c.p.p.</b></p> <p><b>Art. 256. Doveri di esibizione e segreti.</b></p> <p>1. Le persone indicate negli articoli 200 e 201 devono consegnare immediatamente all'autorità giudiziaria, che ne faccia richiesta, gli atti e i documenti, anche in originale se così è ordinato, nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto, e ogni altra cosa esistente presso di esse per ragioni del loro ufficio, incarico, ministero, professione o arte, salvo che dichiarino per iscritto che si tratti di</p>

<p>provider's possession or control.</p> <p>2 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p> <p>3 For the purpose of this article, the term "subscriber information" means any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:</p> <ul style="list-style-type: none"> <li>a the type of communication service used, the technical provisions taken thereto and the period of service;</li> <li>b the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;</li> <li>c any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement.</li> </ul>	<p>segreto di Stato ovvero di segreto inerente al loro ufficio o professione.</p> <p>Article 18 (1) lit. b is not expressly covered.</p> <p>Any provision defines the term "<i>subscriber information</i>" as required by art. 18, para 3 CoC.</p>
<p><b>Article 19 – Search and seizure of stored computer data</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:</p> <ul style="list-style-type: none"> <li>a a computer system or part of it and computer data stored therein; and</li> <li>b a computer-data storage medium in which computer data may be stored</li> </ul> <p style="padding-left: 40px;">in its territory.</p> <p>2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:</p>	<p><b>Article 19 (1) is covered by art. 247, paragraph 1bis c.p.p. Art. 247.Casi e forme delle perquisizioni.</b></p> <p>1.Quando vi è fondato motivo di ritenere che taluno occulti sulla persona il corpo del reato o cose pertinenti al reato, è disposta perquisizione personale. Quando vi è fondato motivo di ritenere che tali cose si trovino in un determinato luogo ovvero che in esso possa eseguirsi l'arresto dell'imputato o dell'evaso, è disposta perquisizione locale.</p> <p>1-bis.Quando vi e' fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione". Possono essere esaminati secondo la novella del secondo comma dell'articolo 248 «presso banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici.</p> <p>2. La perquisizione è disposta con decreto motivato.</p> <p>3. L'autorità giudiziaria può procedere personalmente ovvero disporre che l'atto sia compiuto da ufficiali di polizia giudiziaria delegati con lo stesso decreto.</p> <p><b>Article 19 (3) is covered by art. 250, 254bis and art. 260, paragraph 2 c.p.p.</b></p>

<p>a seize or similarly secure a computer system or part of it or a computer-data storage medium;</p> <p>b make and retain a copy of those computer data;</p> <p>c maintain the integrity of the relevant stored computer data;</p> <p>d render inaccessible or remove those computer data in the accessed computer system.</p> <p>4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.</p> <p>5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p><b>Art. 254-bis. Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni.</b></p> <p>1. L'autorità giudiziaria, quando dispone il sequestro, presso i fornitori di servizi informatici, telematici o di telecomunicazioni, dei dati da questi detenuti, compresi quelli di traffico o di ubicazione, può stabilire, per esigenze legate alla regolare fornitura dei medesimi servizi, che la loro acquisizione avvenga mediante copia di essi su adeguato supporto, con una procedura che assicuri la conformità dei dati acquisiti a quelli originali e la loro immutabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali.</p> <p><b>Art. 19(4) CoC is not expressly covered.</b></p>
<p><b>Article 20 – Real-time collection of traffic data</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to:</p> <p>a collect or record through the application of technical means on the territory of that Party, and</p> <p>b compel a service provider, within its existing technical capability:</p> <p>i to collect or record through the application of technical means on the territory of that Party; or</p> <p>ii to co-operate and assist the competent authorities in the collection or recording of, traffic data, in real-time, associated with specified communications in its territory transmitted by means of a computer system.</p> <p>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of traffic data associated with specified communications transmitted in its territory, through the application of technical means on that territory.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the</p>	<p><b>Art. 20 CoC is partially covered by art. 132, paragraph 4ter, quarter D.lgs. 196/2003.</b></p>



<p>execution of any power provided for in this article and any information relating to it.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	
<p><b>Article 21 – Interception of content data</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary, in relation to a range of serious offences to be determined by domestic law, to empower its competent authorities to:</p> <p>a collect or record through the application of technical means on the territory of that Party, and</p> <p>b compel a service provider, within its existing technical capability:</p> <p>    i to collect or record through the application of technical means on the territory of that Party, or</p> <p>    ii to co-operate and assist the competent authorities in the collection or recording of, content data, in real-time, of specified communications in its territory transmitted by means of a computer system.</p> <p>2 Where a Party, due to the established principles of its domestic legal system, cannot adopt the measures referred to in paragraph 1.a, it may instead adopt legislative and other measures as may be necessary to ensure the real-time collection or recording of content data on specified communications in its territory through the application of technical means on that territory.</p> <p>3 Each Party shall adopt such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of the execution of any power provided for in this article and any information relating to it.</p> <p>4 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.</p>	<p><b>Art. 21 CoC is partially covered by art. 266bis c.p.p.</b></p> <p>Art. 266bis c.p.p does not refer expressly to the interception of content data. It does not provide for the possibility to compel a service provider, within its existing technical capability, as established by art. 21, lit. b CoC.</p>
<p><b>Section 3 – Jurisdiction</b></p>	
<p><b>Article 22 – Jurisdiction</b></p> <p>1 Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:</p> <p>a in its territory; or</p>	<p><b>Art. 6, 7, 9, 10 c.p. (General provisions of Criminal Code)</b></p> <p><b>Art. 6. Reati commessi nel territorio dello Stato.</b></p> <p>Chiunque commette un reato nel territorio dello Stato è punito secondo la legge italiana.</p> <p>Il reato si considera commesso nel territorio dello Stato , quando l'azione o l'omissione, che lo costituisce, è ivi avvenuta in tutto o in parte, ovvero si è ivi</p>

<p>b on board a ship flying the flag of that Party; or</p> <p>c on board an aircraft registered under the laws of that Party; or</p> <p>d by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.</p> <p>2 Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof.</p> <p>3 Each Party shall adopt such measures as may be necessary to establish jurisdiction over the offences referred to in Article 24, paragraph 1, of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him or her to another Party, solely on the basis of his or her nationality, after a request for extradition.</p> <p>4 This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law.</p> <p>When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.</p>	<p>verificato l'evento che è la conseguenza dell'azione od omissione.</p> <p><b>Art. 7. Reati commessi all'estero.</b> E' punito secondo la legge italiana il cittadino o lo straniero che commette in territorio estero taluno dei seguenti reati:</p> <ol style="list-style-type: none"> <li>1. delitti contro la personalità dello Stato italiano;</li> <li>2. delitti di contraffazione del sigillo dello Stato e di uso di tale sigillo contraffatto;</li> <li>3. delitti di falsità in monete aventi corso legale nel territorio dello Stato, o in valori di bollo o in carte di pubblico credito italiano;</li> <li>4. delitti commessi da pubblici ufficiali a servizio dello Stato, abusando dei poteri o violando i doveri inerenti alle loro funzioni;</li> <li>5. ogni altro reato per il quale speciali disposizioni di legge o convenzioni internazionali stabiliscono l'applicabilità della legge penale italiana.</li> </ol> <p>Agli effetti della legge penale, è delitto politico ogni delitto, che offende un interesse politico dello Stato, ovvero un diritto politico del cittadino. E' altresì considerato delitto politico il delitto comune determinato, in tutto o in parte, da motivi politici.</p> <p><b>Art. 9. Delitto comune del cittadino all'estero.</b> Il cittadino, che, fuori dei casi indicati nei due articoli precedenti, commette in territorio estero un delitto per il quale la legge italiana stabilisce la pena di morte o l'ergastolo, o la reclusione non inferiore nel minimo a tre anni, è punito secondo la legge medesima, sempre che si trovi nel territorio dello Stato. Se si tratta di delitto per il quale è stabilita una pena restrittiva della libertà personale di minore durata, il colpevole è punito a richiesta del ministro della giustizia ovvero a istanza, o a querela della persona offesa.</p> <p>Nei casi preveduti dalle disposizioni precedenti, qualora si tratti di delitto commesso a danno delle Comunità europee, di uno Stato estero o di uno straniero, il colpevole è punito a richiesta del ministro della giustizia, sempre che l'estradizione di lui non sia stata concessa, ovvero non sia stata accettata dal Governo dello Stato in cui egli ha commesso il delitto.</p> <p><b>Art. 10. Delitto comune dello straniero all'estero.</b> Lo straniero, che, fuori dei casi indicati negli articoli 7 e 8, commette in territorio estero, a danno dello Stato o di un cittadino, un delitto per il quale la legge italiana stabilisce la pena di morte o l'ergastolo, o la reclusione non inferiore nel minimo a un anno, è punito secondo la legge medesima, sempre che si trovi nel territorio dello Stato, e vi sia richiesta del ministro della giustizia, ovvero istanza o querela della persona offesa.</p>
--	---

	<p>Se il delitto è commesso a danno delle Comunità europee, di uno Stato estero o di uno straniero, il colpevole è punito secondo la legge italiana, a richiesta del ministro della giustizia, sempre che:</p> <ol style="list-style-type: none"> <li>1. si trovi nel territorio dello Stato;</li> <li>2. si tratti di delitto per il quale è stabilita la pena di morte o dell'ergastolo, ovvero della reclusione non inferiore nel minimo a tre anni;</li> <li>3. l'estradizione di lui non sia stata concessa, ovvero non sia stata accettata dal Governo dello Stato in cui egli ha commesso il delitto, o da quello dello Stato a cui egli appartiene.</li> </ol>
<b>Chapter III – International co-operation</b>	
<p><b>Article 24 – Extradition</b></p> <p>1 a This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 through 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty.</p> <p>b Where a different minimum penalty is to be applied under an arrangement agreed on the basis of uniform or reciprocal legislation or an extradition treaty, including the European Convention on Extradition (ETS No. 24), applicable between two or more parties, the minimum penalty provided for under such arrangement or treaty shall apply.</p> <p>2 The criminal offences described in paragraph 1 of this article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.</p> <p>3 If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this article.</p> <p>4 Parties that do not make extradition conditional on the existence of a</p>	<p>Art. 13 c.p. and art. 697 ss. c.p.p.</p>

treaty shall recognise the criminal offences referred to in paragraph 1 of this article as extraditable offences between themselves.

5 Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6 If extradition for a criminal offence referred to in paragraph 1 of this article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as for any other offence of a comparable nature under the law of that Party.

7 a Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and address of each authority responsible for making or receiving requests for extradition or provisional arrest in the absence of a treaty.

b The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure

**Article 25 – General principles relating to mutual assistance**

1 The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.

2 Each Party shall also adopt such legislative and other measures as may be necessary to carry out the obligations set forth in Articles 27 through 35.

3 Each Party may, in urgent circumstances, make requests for mutual assistance or communications related thereto by expedited means of communication, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication (including the use

**Art. 696 and art. 723 ss. c.p.p.**

**Art. 696. Prevalenza delle convenzioni e del diritto internazionale generale.**

1. Le estradizioni, le rogatorie internazionali, gli effetti delle sentenze penali straniere, l'esecuzione all'estero delle sentenze penali italiane e gli altri rapporti con le autorità straniere, relativi all'amministrazione della giustizia in materia penale, sono disciplinati dalle norme della Convenzione europea di assistenza giudiziaria in materia firmata a Strasburgo il 20 aprile 1959 e dalle altre norme delle convenzioni internazionali in vigore per lo Stato e dalle norme di diritto internazionale generale.

2. Se tali norme mancano o non dispongono diversamente, si applicano le norme che seguono.

<p>of encryption, where necessary), with formal confirmation to follow, where required by the requested Party. The requested Party shall accept and respond to the request by any such expedited means of communication.</p> <p>4 Except as otherwise specifically provided in articles in this chapter, mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse co-operation. The requested Party shall not exercise the right to refuse mutual assistance in relation to the offences referred to in Articles 2 through 11 solely on the ground that the request concerns an offence which it considers a fiscal offence.</p> <p>5 Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominate the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.</p>	<p><b>Art. 723. Poteri del ministro di grazia e giustizia.</b></p> <p>1. Il ministro di grazia e giustizia dispone che si dia corso alla rogatoria di un'autorità straniera per comunicazioni, notificazioni e per attività di acquisizione probatoria, salvo che ritenga che gli atti richiesti compromettano la sovranità, la sicurezza o altri interessi essenziali dello Stato.</p> <p>2. Il ministro non dà corso alla rogatoria quando risulta evidente che gli atti richiesti sono espressamente vietati dalla legge o sono contrari ai principi fondamentali dell'ordinamento giuridico italiano. Il ministro non dà altresì corso alla rogatoria quando vi sono fondate ragioni per ritenere che considerazioni relative alla razza, alla religione, al sesso, alla nazionalità, alla lingua, alle opinioni politiche o alle condizioni personali o sociali possano influire negativamente sullo svolgimento o sull'esito del processo e non risulta che l'imputato abbia liberamente espresso il suo consenso alla rogatoria.</p> <p>3. Nei casi in cui la rogatoria ha ad oggetto la citazione di un testimone, di un perito o di un imputato davanti all'autorità giudiziaria straniera, il ministro di grazia e giustizia non dà corso alla rogatoria quando lo Stato richiedente non offre idonea garanzia in ordine all'immunità della persona citata.</p> <p>4. Il ministro ha inoltre facoltà di non dare corso alla rogatoria quando lo Stato richiedente non dia idonee garanzie di reciprocità.</p>
<p><b>Article 26 – Spontaneous information</b></p> <p>1 A Party may, within the limits of its domestic law and without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for co-operation by that Party under this chapter.</p> <p>2 Prior to providing such information, the providing Party may request that it be kept confidential or only used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.</p>	

**Article 27 – Procedures pertaining to mutual assistance requests in the absence of applicable international agreements**

1 Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and requested Parties, the provisions of paragraphs 2 through 9 of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 a Each Party shall designate a central authority or authorities responsible for sending and answering requests for mutual assistance, the execution of such requests or their transmission to the authorities competent for their execution.

b The central authorities shall communicate directly with each other;

c Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph;

d The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3 Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party.

4 The requested Party may, in addition to the grounds for refusal established in Article 25, paragraph 4, refuse assistance if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5 The requested Party may postpone action on a request if such action would prejudice criminal investigations or proceedings conducted by its authorities.

6 Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

**Art. 696 c.p.p. and art. 723 ss. c.p.p.**

**Art. 696. Prevalenza delle convenzioni e del diritto internazionale generale.**

1. Le estradizioni, le rogatorie internazionali, gli effetti delle sentenze penali straniere, l'esecuzione all'estero delle sentenze penali italiane e gli altri rapporti con le autorità straniere, relativi all'amministrazione della giustizia in materia penale, sono disciplinati dalle norme della Convenzione europea di assistenza giudiziaria in materia firmata a Strasburgo il 20 aprile 1959 e dalle altre norme delle convenzioni internazionali in vigore per lo Stato e dalle norme di diritto internazionale generale.

2. Se tali norme mancano o non dispongono diversamente, si applicano le norme che seguono.

**Art. 723. Poteri del ministro di grazia e giustizia.**

1. Il ministro di grazia e giustizia dispone che si dia corso alla rogatoria di un'autorità straniera per comunicazioni, notificazioni e per attività di acquisizione probatoria, salvo che ritenga che gli atti richiesti compromettano la sovranità, la sicurezza o altri interessi essenziali dello Stato.

2. Il ministro non dà corso alla rogatoria quando risulta evidente che gli atti richiesti sono espressamente vietati dalla legge o sono contrari ai principi fondamentali dell'ordinamento giuridico italiano. Il ministro non dà altresì corso alla rogatoria quando vi sono fondate ragioni per ritenere che considerazioni relative alla razza, alla religione, al sesso, alla nazionalità, alla lingua, alle opinioni politiche o alle condizioni personali o sociali possano influire negativamente sullo svolgimento o sull'esito del processo e non risulta che l'imputato abbia liberamente espresso il suo consenso alla rogatoria.

3. Nei casi in cui la rogatoria ha ad oggetto la citazione di un testimone, di un perito o di un imputato davanti all'autorità giudiziaria straniera, il ministro di grazia e giustizia non dà corso alla rogatoria quando lo Stato richiedente non offre idonea garanzia in ordine all'immunità della persona citata.

4. Il ministro ha inoltre facoltà di non dare corso alla rogatoria quando lo Stato richiedente non dia idonee garanzie di reciprocità

7 The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. Reasons shall be given for any refusal or postponement of the request. The requested Party shall also inform the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8 The requesting Party may request that the requested Party keep confidential the fact of any request made under this chapter as well as its subject, except to the extent necessary for its execution. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

9 a In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases, a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

b Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

c Where a request is made pursuant to sub-paragraph a. of this article and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

d Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

e Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

**Article 28 – Confidentiality and limitation on use**

1 When there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation in force between the requesting and the requested Parties, the provisions of this article shall apply. The provisions of this article shall not apply where such treaty, arrangement or legislation

exists, unless the Parties concerned agree to apply any or all of the remainder of this article in lieu thereof.

2 The requested Party may make the supply of information or material in response to a request dependent on the condition that it is:

- a kept confidential where the request for mutual legal assistance could not be complied with in the absence of such condition, or
- b not used for investigations or proceedings other than those stated in the request.

3 If the requesting Party cannot comply with a condition referred to in paragraph 2, it shall promptly inform the other Party, which shall then determine whether the information should nevertheless be provided. When the requesting Party accepts the condition, it shall be bound by it.

4 Any Party that supplies information or material subject to a condition referred to in paragraph 2 may require the other Party to explain, in relation to that condition, the use made of such information or material.

**Article 29 – Expedited preservation of stored computer data**

1 A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2 A request for preservation made under paragraph 1 shall specify:

- a the authority seeking the preservation;
- b the offence that is the subject of a criminal investigation or proceedings and a brief summary of the related facts;
- c the stored computer data to be preserved and its relationship to the offence;
- d any available information identifying the custodian of the stored computer data or the location of the computer system;
- e the necessity of the preservation; and
- f that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the stored computer data.

3 Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to

**See art. 4ter D.lgs. 196/2003**



a request, dual criminality shall not be required as a condition to providing such preservation.

4 A Party that requires dual criminality as a condition for responding to a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of stored data may, in respect of offences other than those established in accordance with Articles 2 through 11 of this Convention, reserve the right to refuse the request for preservation under this article in cases where it has reasons to believe that at the time of disclosure the condition of dual criminality cannot be fulfilled.

5 In addition, a request for preservation may only be refused if:

a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence, or

b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

6 Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

4 Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than sixty days, in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such a request, the data shall continue to be preserved pending a decision on that request.

**Article 30 – Expedited disclosure of preserved traffic data**

1 Where, in the course of the execution of a request made pursuant to Article 29 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in another State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data to identify that service provider and the path through which the communication was transmitted.

2 Disclosure of traffic data under paragraph 1 may only be withheld if:

<p>a the request concerns an offence which the requested Party considers a political offence or an offence connected with a political offence; or</p> <p>b the requested Party considers that execution of the request is likely to prejudice its sovereignty, security, <i>ordre public</i> or other essential interests.</p>	
<p><b>Article 31 – Mutual assistance regarding accessing of stored computer data</b></p> <p>1 A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 29.</p> <p>2 The requested Party shall respond to the request through the application of international instruments, arrangements and laws referred to in Article 23, and in accordance with other relevant provisions of this chapter.</p> <p>3 The request shall be responded to on an expedited basis where:</p> <p>a there are grounds to believe that relevant data is particularly vulnerable to loss or modification; or</p> <p>b the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.</p>	
<p><b>Article 32 – Trans-border access to stored computer data with consent or where publicly available</b></p> <p>A Party may, without the authorisation of another Party:</p> <p>a access publicly available (open source) stored computer data, regardless of where the data is located geographically; or</p> <p>b access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.</p>	
<p><b>Article 33 – Mutual assistance in the real-time collection of traffic data</b></p> <p>1 The Parties shall provide mutual assistance to each other in the real-time collection of traffic data associated with specified communications in their territory transmitted by means of a computer system. Subject to the provisions of paragraph 2, this assistance shall be governed by the conditions and procedures provided for under domestic law.</p> <p>2 Each Party shall provide such assistance at least with respect to criminal</p>	

<p>offences for which real-time collection of traffic data would be available in a similar domestic case.</p>	
<p><b>Article 34 – Mutual assistance regarding the interception of content data</b>  The Parties shall provide mutual assistance to each other in the real-time collection or recording of content data of specified communications transmitted by means of a computer system to the extent permitted under their applicable treaties and domestic laws.</p>	
<p><b>Article 35 – 24/7 Network</b>  1 Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:  a the provision of technical advice;  b the preservation of data pursuant to Articles 29 and 30;  c the collection of evidence, the provision of legal information, and locating of suspects.  2 a A Party’s point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.   b If the point of contact designated by a Party is not part of that Party’s authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.   3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.</p>	<p>Minister of Interior, in accordance with Minister of Justice, establishes a 24/7 contact point (see art. 13 Ratification Law).</p> <p>Italy is a member of the 24/7 Network of the “G8 High-Tech Crime Subgroup” and of the ICPO Interpol.</p>
<p><b>Article 42 – Reservations</b>  By a written notification addressed to the Secretary General of the Council of Europe, any State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, declare that it</p>	

avails itself of the reservation(s) provided for in Article 4, paragraph 2, Article 6, paragraph 3, Article 9, paragraph 4, Article 10, paragraph 3, Article 11, paragraph 3, Article 14, paragraph 3, Article 22, paragraph 2, Article 29, paragraph 4, and Article 41, paragraph 1. No other reservation may be made.