SENATO DELLA REPUBBLICA

XV LEGISLATURA

N. 2012

DISEGNO DI LEGGE

presentato dal Ministro degli affari esteri

(D'ALEMA)

dal Ministro della giustizia

(MASTELLA)

dal Ministro delle comunicazioni

(GENTILONI SILVERI)

e dal Ministro per le riforme e le innovazioni nella pubblica amministrazione

(NICOLAIS)

di concerto col Ministro dell'interno

(AMATO)

col Ministro della difesa

(PARISI)

e col Ministro dell'economia e delle finanze

(PADOA-SCHIOPPA)

(V. *Stampato Camera n.* **2807**)

approvato dalla Camera dei deputati il 20 febbraio 2008

Trasmesso dal Presidente della Camera dei deputati alla Presidenza il 22 febbraio 2008

Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno

---

TIPOGRAFIA DEL SENATO (700)

DISEGNO DI LEGGE

CAPO I

RATIFICA ED ESECUZIONE

Art. 1.

(Autorizzazione alla ratifica)

1. Il Presidente della Repubblica è autorizzato a ratificare la Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, di seguito denominata «Convenzione».

Art. 2.

(Ordine di esecuzione)

1. Piena e intera esecuzione è data alla Convenzione, a decorrere dalla data della sua entrata in vigore in conformità a quanto disposto dall'articolo 36 della Convenzione stessa.

CAPO II

MODIFICHE AL CODICE PENALE E AL DECRETO LEGISLATIVO 8 GIUGNO 2001, N. 231

Art. 3.

(Modifiche al titolo VII del libro secondo del codice penale)

1. All'articolo 491-*bis* del codice penale sono apportate le seguenti modificazioni:

a) al primo periodo, dopo la parola: «privato» sono inserite le seguenti: «avente efficacia probatoria»;

b) il secondo periodo è soppresso.

2. Dopo l'articolo 495 del codice penale è inserito il seguente:

«Art. 495-*bis*. – *(Falsa dichiarazione o attestazione al certificatore di firma elettronica sull'identità o su qualità personali proprie o di altri)*. – Chiunque dichiara o attesta falsamente al soggetto che presta servizi di certificazione delle firme elettroniche l'identità o lo stato o altre qualità della propria o dell'altrui persona è punito con la reclusione fino ad un anno».

Art. 4.

(Modifica al titolo XII del libro secondo del codice penale)

1. L'articolo 615-*quinquies* del codice penale è sostituito dal seguente:

«Art. 615-*quinquies*. – *(Diffusione di apparecchiature, dispositivi o programmi informatici diretti a danneggiare o interrompere un sistema informatico o telematico)*. – Chiunque, allo scopo di danneggiare illecitamente un sistema informatico o telematico, le informazioni, i dati o i programmi in esso contenuti o ad esso pertinenti ovvero di favorire l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, si procura, produce, riproduce, importa, diffonde, comunica, consegna o, comunque, mette a disposizione di altri apparecchiature, dispositivi o programmi informatici, è punito con la reclusione fino a due anni e con la multa sino a euro 10.329».

Art. 5.

(Modifiche al titolo XIII del libro secondo del codice penale)

1. L'articolo 635-*bis* del codice penale è sostituito dal seguente:

«Art. 635-*bis*. – *(Danneggiamento di informazioni, dati e programmi informatici)*.

– Salvo che il fatto costituisca più grave reato, chiunque distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui è punito, a querela della persona offesa, con la reclusione da sei mesi a tre 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 della reclusione da uno a quattro anni e si procede d'ufficio».

2. Dopo l'articolo 635-*bis* del codice penale sono inseriti i seguenti:

«Art. 635-*ter*. – *(Danneggiamento di informazioni, dati e programmi informatici utilizzati dallo Stato o da altro ente pubblico o comunque di pubblica utilità).* – Salvo che il fatto costituisca più grave reato, chiunque commette un fatto diretto a distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità, è punito con la reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione, il deterioramento, la cancellazione, l'alterazione o la soppressione delle informazioni, dei dati o dei programmi informatici, la pena è della reclusione da tre a otto 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.

Art. 635-*quater*. – *(Danneggiamento di sistemi informatici o telematici).* – Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-*bis*, 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 fun-

zionamento 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.

Art. 635-*quinquies*. – *(Danneggiamento di sistemi informatici o telematici di pubblica utilità)*. – Se il fatto di cui all'articolo 635-*quater* è diretto a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento, la pena è della reclusione da uno a quattro anni.

Se dal fatto deriva la distruzione o il danneggiamento del sistema informatico o telematico di pubblica utilità ovvero se questo è reso, in tutto o in parte, inservibile, la pena è della reclusione da tre a otto 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».

3. Dopo l'articolo 640-*quater* del codice penale è inserito il seguente:

«Art. 640-*quinquies*. – *(Frode informatica del soggetto che presta servizi di certificazione di firma elettronica)*. – Il soggetto che presta servizi di certificazione di firma elettronica, il quale, al fine di procurare a sé o ad altri un ingiusto profitto ovvero di arrecare ad altri danno, viola gli obblighi previsti dalla legge per il rilascio di un certificato qualificato, è punito con la reclusione fino a tre anni e con la multa da 51 a 1.032 euro».

Art. 6.

(Modifiche all'articolo 420 del codice penale)

1. All'articolo 420 del codice penale, il secondo e il terzo comma sono abrogati.

Art. 7.

*(Introduzione dell'articolo 24-*bis *del decreto legislativo 8 giugno 2001, n. 231)*

1. Dopo l'articolo 24 del decreto legislativo 8 giugno 2001, n. 231, è inserito il seguente:

«Art. 24-*bis*. – *(Delitti informatici e trattamento illecito di dati). – 1.* In relazione alla commissione dei delitti di cui agli articoli 615-*ter*, 617-*quater*, 617-*quinquies*, 635-*bis*, 635-*ter*, 635-*quater* e 635-*quinquies* del codice penale, si applica all'ente la sanzione pecuniaria da cento a cinquecento quote.

2. In relazione alla commissione dei delitti di cui agli articoli 615-*quater* e 615-*quinquies* del codice penale, si applica all'ente la sanzione pecuniaria sino a trecento quote.

3. In relazione alla commissione dei delitti di cui agli articoli 491-*bis* e 640-*quinquies* del codice penale, salvo quanto previsto dall'articolo 24 del presente decreto per i casi di frode informatica in danno dello Stato o di altro ente pubblico, si applica all'ente la sanzione pecuniaria sino a quattrocento quote.

4. Nei casi di condanna per uno dei delitti indicati nel comma 1 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere *a)*, *b)* ed *e)*. Nei casi di condanna per uno dei delitti indicati nel comma 2 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere *b)* ed *e)*. Nei casi di condanna per uno dei delitti indicati nel comma 3 si applicano le sanzioni interdittive previste dall'articolo 9, comma 2, lettere *c), d)* ed *e)*».

CAPO III

MODIFICHE AL CODICE DI PROCEDURA PENALE E AL CODICE DI CUI AL DECRETO LEGISLATIVO 30 GIUGNO 2003, N. 196

Art. 8.

(Modifiche al titolo III del libro terzo del codice di procedura penale)

1. All'articolo 244, comma 2, secondo periodo, del codice di procedura penale sono aggiunte, in fine, le seguenti parole: «, anche in relazione a sistemi informatici o telematici, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione».

2. All'articolo 247 del codice di procedura penale, dopo il comma 1 è inserito il seguente:

«*1*-bis. Quando vi è 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».

3. All'articolo 248, comma 2, primo periodo, del codice di procedura penale, le parole: «atti, documenti e corrispondenza presso banche» sono sostituite dalle seguenti: «presso banche atti, documenti e corrispondenza nonché dati, informazioni e programmi informatici».

4. All'articolo 254 del codice di procedura penale sono apportate le seguenti modificazioni:

a) il comma 1 è sostituito dal seguente:

«*1*. Presso coloro che forniscono servizi postali, telegrafici, telematici o di telecomunicazioni è consentito procedere al sequestro

di lettere, pieghi, pacchi, valori, telegrammi e altri oggetti di corrispondenza, anche se inoltrati per via telematica, che l'autorità giudiziaria abbia fondato motivo di ritenere spediti dall'imputato o a lui diretti, anche sotto nome diverso o per mezzo di persona diversa, o che comunque possono avere relazione con il reato»;

b) al comma 2, dopo le parole: «senza aprirli» sono inserite le seguenti: «o alterarli».

5. Dopo l'articolo 254 del codice di procedura penale è inserito il seguente:

«Art. 254-*bis*. – *(Sequestro di dati informatici presso fornitori di servizi informatici, telematici e di telecomunicazioni). – 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 immodificabilità. In questo caso è, comunque, ordinato al fornitore dei servizi di conservare e proteggere adeguatamente i dati originali».

6. All'articolo 256, comma 1, del codice di procedura penale, dopo le parole: «anche in originale se così è ordinato,» sono inserite le seguenti: «nonché i dati, le informazioni e i programmi informatici, anche mediante copia di essi su adeguato supporto,».

7. All'articolo 259, comma 2, del codice di procedura penale, dopo il primo periodo è inserito il seguente: «Quando la custodia riguarda dati, informazioni o programmi informatici, il custode è altresì avvertito dell'obbligo di impedirne l'alterazione o l'accesso da parte di terzi, salva, in quest'ultimo caso, diversa disposizione dell'autorità giudiziaria».

8. All'articolo 260 del codice di procedura penale sono apportate le seguenti modificazioni:

a) al comma 1, dopo le parole: «con altro mezzo» sono inserite le seguenti: «, anche di carattere elettronico o informatico,»;

b) al comma 2 è aggiunto, in fine, il seguente periodo: «Quando si tratta di dati, di informazioni o di programmi informatici, la copia deve essere realizzata su adeguati supporti, mediante procedura che assicuri la conformità della copia all'originale e la sua immodificabilità; in tali casi, la custodia degli originali può essere disposta anche in luoghi diversi dalla cancelleria o dalla segreteria».

Art. 9.

(Modifiche al titolo IV del libro quinto del codice di procedura penale)

1. All'articolo 352 del codice di procedura penale, dopo il comma 1 è inserito il seguente:

«*1*-bis. Nella flagranza del reato, ovvero nei casi di cui al comma 2 quando sussistono i presupposti e le altre condizioni ivi previsti, gli ufficiali di polizia giudiziaria, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione, procedono altresì alla perquisizione di sistemi informatici o telematici, ancorché protetti da misure di sicurezza, quando hanno fondato motivo di ritenere che in questi si trovino occultati dati, informazioni, programmi informatici o tracce comunque pertinenti al reato che possono essere cancellati o dispersi».

2. All'articolo 353 del codice di procedura penale sono apportate le seguenti modificazioni:

a) al comma 2 sono aggiunte, in fine, le seguenti parole: «e l'accertamento del contenuto»;

b) al comma 3, primo periodo, le parole: «lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza» sono sostituite dalle seguenti: «lettere, pieghi, pacchi, valori, telegrammi o altri oggetti di corrispondenza, anche se in forma elettronica o se inoltrati per via telematica,» e dopo le parole: «servizio postale» sono inserite le seguenti: «, telegrafico, telematico o di telecomunicazione».

3. All'articolo 354, comma 2, del codice di procedura penale, dopo il primo periodo è inserito il seguente: «In relazione ai dati, alle informazioni e ai programmi informatici o ai sistemi informatici o telematici, gli ufficiali della polizia giudiziaria adottano, altresì, le misure tecniche o impartiscono le prescrizioni necessarie ad assicurarne la conservazione e ad impedirne l'alterazione e l'accesso e provvedono, ove possibile, alla loro immediata duplicazione su adeguati supporti, mediante una procedura che assicuri la conformità della copia all'originale e la sua immodificabilità».

Art. 10.

(Modifiche all'articolo 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196)

1. Dopo il comma 4-*bis* dell'articolo 132 del codice in materia di protezione dei dati personali, di cui al decreto legislativo 30 giugno 2003, n. 196, sono inseriti i seguenti:

«*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 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.

4-quater. Il fornitore o l'operatore di servizi informatici o telematici cui è rivolto l'ordine previsto dal comma 4-*ter* deve ottemperarvi senza ritardo, fornendo immediatamente all'autorità richiedente l'assicurazione dell'adempimento. Il fornitore o l'operatore di servizi informatici o telematici è tenuto a mantenere il segreto relativamente all'ordine ricevuto e alle attività conseguentemente svolte per il periodo indicato dall'autorità. In caso di violazione dell'obbligo si applicano, salvo che il fatto costituisca più grave reato, le disposizioni dell'articolo 326 del codice penale.

4-quinquies. I provvedimenti adottati ai sensi del comma 4-*ter* sono comunicati per iscritto, senza ritardo e comunque entro quarantotto ore dalla notifica al destinatario, al pubblico ministero del luogo di esecuzione il quale, se ne ricorrono i presupposti, li convalida. In caso di mancata convalida, i provvedimenti assunti perdono efficacia».

Art. 11.

(Competenza)

1. All'articolo 51 del codice di procedura penale è aggiunto, in fine, il seguente comma:

«*3*-quinquies. Quando si tratta di procedimenti per i delitti, consumati o tentati, di cui agli articoli 600-*bis*, 600-*ter*, 600-*quater*, 600-*quater*.1, 600-*quinquies*, 615-*ter*, 615-*quater*, 615-*quinquies*, 617-*bis*, 617-*ter*, 617-*quater*, 617-*quinquies*, 617-*sexies*, 635-*bis*, 635-*ter*, 635-*quater*, 640-*ter* e 640-*quinquies* del codice penale, le funzioni indicate nel comma 1, lettera *a)*, del presente articolo sono attribuite all'ufficio del pubblico ministero presso il tribunale del capoluogo del distretto nel cui ambito ha sede il giudice competente».

Art. 12.

(Fondo per il contrasto della pedopornografia su internet *e per la protezione delle infrastrutture informatiche di interesse nazionale)*

1. Per le esigenze connesse al funzionamento del Centro nazionale per il contrasto della pedopornografia sulla rete INTERNET, di cui all'articolo 14-*bis* della legge 3 agosto 1998, n. 269, e dell'organo del Ministero dell'interno per la sicurezza e per la regolarità dei servizi di telecomunicazione per le esigenze relative alla protezione informatica delle infrastrutture critiche informatizzate di interesse nazionale, di cui all'articolo 7-*bis* del decreto-legge 27 luglio 2005, n. 144, convertito, con modificazioni, dalla legge 31 luglio 2005, n. 155, è istituito, nello stato di previsione del Ministero dell'interno, un fondo con una dotazione di 2 milioni di euro annui a decorrere dall'anno 2008.

2. Agli oneri derivanti dal presente articolo, pari a 2 milioni di euro annui a decor-

rere dall'anno 2008, si provvede mediante corrispondente riduzione dello stanziamento iscritto, ai fini del bilancio triennale 2008-2010, nell'ambito del fondo speciale di parte corrente dello stato di previsione del Ministero dell'economia e delle finanze per l'anno 2008, allo scopo parzialmente utilizzando l'accantonamento relativo al Ministero della giustizia.

3. Il Ministro dell'economia e delle finanze è autorizzato ad apportare, con propri decreti, le occorrenti variazioni di bilancio.

CAPO IV

DISPOSIZIONI FINALI

Art. 13.

(Norma di adeguamento)

1. L'autorità centrale ai sensi degli articoli 24, paragrafo 7, e 27, paragrafo 2, della Convenzione è il Ministro della giustizia.

2. Il Ministro dell'interno, di concerto con il Ministro della giustizia, individua il punto di contatto di cui all'articolo 35 della Convenzione.

Art. 14.

(Entrata in vigore)

1. La presente legge entra in vigore il giorno successivo a quello della sua pubblicazione nella *Gazzetta Ufficiale*.

CONVENTION ON CYBERCRIME

CONVENTION SUR LA CYBERCRIMINALITÉ

Préambule

Les Etats membres du Conseil de l'Europe et les autres Etats signataires,

Considérant que le but du Conseil de l'Europe est de réaliser une union plus étroite entre ses membres;

Reconnaissant l'intérêt d'intensifier la coopération avec les autres Etats parties à la Convention;

Convaincus de la nécessité de mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyberespace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale;

Conscients des profonds changements engendrés par la numérisation, la convergence et la mondialisation permanente des réseaux informatiques;

Préoccupés par le risque que les réseaux informatiques et l'information électronique soient utilisés également pour commettre des infractions pénales et que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux;

Reconnaissant la nécessité d'une coopération entre les Etats et l'industrie privée dans la lutte contre la cybercriminalité, et le besoin de protéger les intérêts légitimes dans l'utilisation et le développement des technologies de l'information;

Estimant qu'une lutte bien menée contre la cybercriminalité requiert une coopération internationale en matière pénale accrue, rapide et efficace;

Convaincus que la présente Convention est nécessaire pour prévenir les actes portant atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes informatiques, des réseaux et des données, ainsi que l'usage frauduleux de tels systèmes, réseaux et données, en assurant l'incrimination de ces comportements, tels que décrits dans la présente Convention, et l'adoption de pouvoirs suffisants pour permettre une lutte efficace contre ces infractions pénales, en en facilitant la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international, et en prévoyant des dispositions matérielles en vue d'une coopération internationale rapide et fiable;

Gardant à l'esprit la nécessité de garantir un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits de l'homme fondamentaux, tels que garantis dans la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950), dans le Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ainsi que dans d'autres conventions internationales applicables en matière de

droits de l'homme, qui réaffirment le droit à ne pas être inquiété pour ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontière, ainsi que le droit au respect de la vie privée ;

Conscients également du droit à la protection des données personnelles, tel que spécifié, par exemple, par la Convention de 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Considérant la Convention des Nations Unies relative aux droits de l'enfant (1989) et la Convention de l'Organisation internationale du travail sur les pires formes de travail des enfants (1999) ;

Tenant compte des conventions existantes du Conseil de l'Europe sur la coopération en matière pénale, ainsi que d'autres traités similaires conclus entre les Etats membres du Conseil de l'Europe et d'autres Etats, et soulignant que la présente Convention a pour but de les compléter en vue de rendre plus efficaces les enquêtes et les procédures pénales portant sur des infractions pénales en relation avec des systèmes et des données informatiques, ainsi que de permettre la collecte des preuves électroniques d'une infraction pénale ;

Se félicitant des récentes initiatives destinées à améliorer la compréhension et la coopération internationales aux fins de la lutte contre la criminalité dans le cyberespace, notamment des actions menées par les Nations Unies, l'OCDE, l'Union européenne et le G8 ;

Rappelant les Recommandations du Comité des Ministres n° R (85) 10 concernant l'application pratique de la Convention européenne d'entraide judiciaire en matière pénale relative aux commissions rogatoires pour la surveillance des télécommunications, n° R (88) 2 sur des mesures visant à combattre la piraterie dans le domaine du droit d'auteur et des droits voisins, n° R (87) 15 visant à réglementer l'utilisation de données à caractère personnel dans le secteur de la police, n° R (95) 4 sur la protection des données à caractère personnel dans le domaine des services de télécommunication, eu égard notamment aux services téléphoniques, et n° R (89) 9 sur la criminalité en relation avec l'ordinateur, qui indique aux législateurs nationaux des principes directeurs pour définir certaines infractions informatiques, ainsi que n° R (95) 13 relative aux problèmes de procédure pénale liés à la technologie de l'information ;

Eu égard à la Résolution n° 1, adoptée par les ministres européens de la Justice lors de leur 21e Conférence (Prague, 10 et 11 juin 1997), qui recommande au Comité des Ministres de soutenir les activités concernant la cybercriminalité menées par le Comité européen pour les problèmes criminels (CDPC) afin de rapprocher les législations pénales nationales et de permettre l'utilisation de moyens d'investigation efficaces en matière d'infractions informatiques, ainsi qu'à la Résolution n° 3, adoptée lors de la 23e Conférence des ministres européens de la Justice (Londres, 8 et 9 juin 2000), qui encourage les parties aux négociations à poursuivre leurs efforts afin de trouver des solutions permettant au plus grand nombre d'Etats d'être parties à la Convention et qui reconnaît la nécessité de disposer d'un mécanisme rapide et efficace de coopération internationale qui tienne dûment compte des exigences spécifiques de la lutte contre la cybercriminalité ;

Prenant également en compte le plan d'action adopté par les chefs d'Etat et de gouvernement du Conseil de l'Europe à l'occasion de leur 2e Sommet (Strasbourg, 10 et 11 octobre 1997) afin de trouver des réponses communes au développement des nouvelles technologies de l'information, fondées sur les normes et les valeurs du Conseil de l'Europe,

Sont convenus de ce qui suit:

Chapitre I – Terminologie

Article 1 – Définitions

Aux fins de la présente Convention,

a l'expression «système informatique» désigne tout dispositif isolé ou ensemble de dispositifs interconnectés ou apparentés, qui assure ou dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données;

b l'expression «données informatiques» désigne toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire en sorte qu'un système informatique exécute une fonction;

c l'expression «fournisseur de services» désigne:

i toute entité publique ou privée qui offre aux utilisateurs de ses services la possibilité de communiquer au moyen d'un système informatique, et

ii toute autre entité traitant ou stockant des données informatiques pour ce service de communication ou ses utilisateurs.

d «données relatives au trafic» désigne toutes données ayant trait à une communication passant par un système informatique, produites par ce dernier en tant qu'élément de la chaîne de communication, indiquant l'origine, la destination, l'itinéraire, l'heure, la date, la taille et la durée de la communication ou le type de service sous-jacent.

Chapitre II – Mesures à prendre au niveau national

Section 1 – Droit pénal matériel

Titre 1 – Infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques

Article 2 – Accès illégal

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'accès intentionnel et sans droit à tout ou partie d'un système informatique. Une Partie peut exiger que l'infraction soit commise en violation des mesures de sécurité, dans l'intention d'obtenir des données informatiques ou dans une autre intention délictueuse, ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 3 – Interception illégale

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'interception intentionnelle et sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique, y compris les émissions électromagnétiques provenant d'un système informatique transportant de telles données informatiques. Une Partie peut exiger que l'infraction soit commise dans une intention délictueuse ou soit en relation avec un système informatique connecté à un autre système informatique.

Article 4 – Atteinte à l'intégrité des données

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait, intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques.

2 Une Partie peut se réserver le droit d'exiger que le comportement décrit au paragraphe 1 entraîne des dommages sérieux.

Article 5 – Atteinte à l'intégrité du système

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques.

Article 6 – Abus de dispositifs

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, lorsqu'elles sont commises intentionnellement et sans droit :

a la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition :

i d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions établies conformément aux articles 2 à 5 ci-dessus ;

ii d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique,

dans l'intention qu'ils soient utilisés afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5 ; et

b la possession d'un élément visé aux paragraphes a.i ou ii ci-dessus, dans l'intention qu'il soit utilisé afin de commettre l'une ou l'autre des infractions visées par les articles 2 à 5. Une Partie peut exiger en droit interne qu'un certain nombre de ces éléments soit détenu pour que la responsabilité pénale soit engagée.

2 Le présent article ne saurait être interprété comme imposant une responsabilité pénale lorsque la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition mentionnées au paragraphe 1 du présent article n'ont pas pour but de commettre une infraction établie conformément aux articles 2 à 5 de la présente Convention, comme dans le cas d'essai autorisé ou de protection d'un système informatique.

3 Chaque Partie peut se réserver le droit de ne pas appliquer le paragraphe 1 du présent article, à condition que cette réserve ne porte pas sur la vente, la distribution ou toute autre mise à disposition des éléments mentionnés au paragraphe 1.a.ii du présent article.

Titre 2 – Infractions informatiques

Article 7 – Falsification informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, l'introduction, l'altération, l'effacement

ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient ou non directement lisibles et intelligibles. Une Partie peut exiger une intention frauduleuse ou une intention délictueuse similaire pour que la responsabilité pénale soit engagée.

Article 8 – Fraude informatique

Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui :

a par toute introduction, altération, effacement ou suppression de données informatiques ;

b par toute forme d'atteinte au fonctionnement d'un système informatique,

dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui.

Titre 3 – Infractions se rapportant au contenu

Article 9 – Infractions se rapportant à la pornographie enfantine

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les comportements suivants lorsqu'ils sont commis intentionnellement et sans droit :

a la production de pornographie enfantine en vue de sa diffusion par le biais d'un système informatique ;

b l'offre ou la mise à disposition de pornographie enfantine par le biais d'un système informatique ;

c la diffusion ou la transmission de pornographie enfantine par le biais d'un système informatique ;

d le fait de se procurer ou de procurer à autrui de la pornographie enfantine par le biais d'un système informatique ;

e la possession de pornographie enfantine dans un système informatique ou un moyen de stockage de données informatiques.

2 Aux fins du paragraphe 1 ci-dessus, le terme « pornographie enfantine » comprend toute matière pornographique représentant de manière visuelle :

a un mineur se livrant à un comportement sexuellement explicite ;

b une personne qui apparaît comme un mineur se livrant à un comportement sexuellement explicite ;

c des images réalistes représentant un mineur se livrant à un comportement sexuellement explicite.

3 Aux fins du paragraphe 2 ci-dessus, le terme « mineur » désigne toute personne âgée de moins de 18 ans. Une Partie peut toutefois exiger une limite d'âge inférieure, qui doit être au minimum de 16 ans.

4 Une Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, les paragraphes 1, alinéas d. et e, et 2, alinéas b. et c.

Titre 4 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

Article 10 – Infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes à la propriété intellectuelle, définies par la législation de ladite Partie, conformément aux obligations que celle-ci a souscrites en application de l'Acte de Paris du 24 juillet 1971 portant révision de la Convention de Berne pour la protection des œuvres littéraires et artistiques, de l'Accord sur les aspects commerciaux des droits de propriété intellectuelle et du traité de l'OMPI sur la propriété intellectuelle, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, les atteintes aux droits connexes définis par la législation de ladite Partie, conformément aux obligations que cette dernière a souscrites en application de la Convention internationale pour la protection des artistes interprètes ou exécutants, des producteurs de phonogrammes et des organismes de radiodiffusion (Convention de Rome), de l'Accord relatif aux aspects commerciaux des droits de propriété intellectuelle et du Traité de l'OMPI sur les interprétations et exécutions, et les phonogrammes, à l'exception de tout droit moral conféré par ces conventions, lorsque de tels actes sont commis délibérément, à une échelle commerciale et au moyen d'un système informatique.

3 Une Partie peut, dans des circonstances bien délimitées, se réserver le droit de ne pas imposer de responsabilité pénale au titre des paragraphes 1 et 2 du présent article, à condition que d'autres recours efficaces soient disponibles et qu'une telle réserve ne porte pas atteinte aux obligations internationales incombant à cette Partie en application des instruments internationaux mentionnés aux paragraphes 1 et 2 du présent article.

Titre 5 – Autres formes de responsabilité et de sanctions

Article 11 – Tentative et complicité

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute complicité lorsqu'elle est commise intentionnellement en vue de la perpétration d'une des infractions établies en application des articles 2 à 10 de la présente Convention, dans l'intention qu'une telle infraction soit commise.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour ériger en infraction pénale, conformément à son droit interne, toute tentative intentionnelle de commettre l'une des infractions établies en application des articles 3 à 5, 7, 8, 9.1.a et c de la présente Convention.

3 Chaque Partie peut se réserver le droit de ne pas appliquer, en tout ou en partie, le paragraphe 2 du présent article.

Article 12 – Responsabilité des personnes morales

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les personnes morales puissent être tenues pour responsables des infractions établies en application

de la présente Convention, lorsqu'elles sont commises pour leur compte par toute personne physique, agissant soit individuellement, soit en tant que membre d'un organe de la personne morale, qui exerce un pouvoir de direction en son sein, fondé :

a sur un pouvoir de représentation de la personne morale ;

b sur une autorité pour prendre des décisions au nom de la personne morale ;

c sur une autorité pour exercer un contrôle au sein de la personne morale.

2 Outre les cas déjà prévus au paragraphe 1 du présent article, chaque Partie adopte les mesures qui se révèlent nécessaires pour s'assurer qu'une personne morale peut être tenue pour responsable lorsque l'absence de surveillance ou de contrôle de la part d'une personne physique mentionnée au paragraphe 1 a rendu possible la commission des infractions établies en application de la présence Convention pour le compte de ladite personne morale par une personne physique agissant sous son autorité.

3 Selon les principes juridiques de la Partie, la responsabilité d'une personne morale peut être pénale, civile ou administrative.

4 Cette responsabilité est établie sans préjudice de la responsabilité pénale des personnes physiques ayant commis l'infraction.

Article 13 – Sanctions et mesures

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour que les infractions pénales établies en application des articles 2 à 11 soient passibles de sanctions effectives, proportionnées et dissuasives, comprenant des peines privatives de liberté.

2 Chaque Partie veille à ce que les personnes morales tenues pour responsables en application de l'article 12 fassent l'objet de sanctions ou de mesures pénales ou non pénales effectives, proportionnées et dissuasives, comprenant des sanctions pécuniaires.

Section 2 – Droit procédural

Titre 1 – Dispositions communes

Article 14 – Portée d'application des mesures du droit de procédure

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour instaurer les pouvoirs et procédures prévus dans la présente section aux fins d'enquêtes ou de procédures pénales spécifiques.

2 Sauf disposition contraire figurant à l'article 21, chaque Partie applique les pouvoirs et procédures mentionnés dans le paragraphe 1 du présent article :

a aux infractions pénales établies conformément aux articles 2 à 11 de la présente Convention ;

b à toutes les autres infractions pénales commises au moyen d'un système informatique ; et

c à la collecte des preuves électroniques de toute infraction pénale.

3 a Chaque Partie peut se réserver le droit de n'appliquer les mesures mentionnées à l'article 20 qu'aux infractions ou catégories d'infractions spécifiées dans la réserve, pour autant que l'éventail de ces infractions ou catégories d'infractions ne soit pas plus réduit que celui des infractions auxquelles elle applique les mesures mentionnées à l'article 21. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée à l'article 20.

b Lorsqu'une Partie, en raison des restrictions imposées par sa législation en vigueur au moment de l'adoption de la présente Convention, n'est pas en mesure d'appliquer les mesures visées aux articles 20 et 21 aux communications transmises dans un système informatique d'un fournisseur de services :

i qui est mis en œuvre pour le bénéfice d'un groupe d'utilisateurs fermé, et

ii qui n'emploie pas les réseaux publics de télécommunication et qui n'est pas connecté à un autre système informatique, qu'il soit public ou privé,

cette Partie peut réserver le droit de ne pas appliquer ces mesures à de telles communications. Chaque Partie envisagera de limiter une telle réserve de manière à permettre l'application la plus large possible de la mesure mentionnée aux articles 20 et 21.

Article 15 – Conditions et sauvegardes

1 Chaque Partie veille à ce que l'instauration, la mise en œuvre et l'application des pouvoirs et procédures prévus dans la présente section soient soumises aux conditions et sauvegardes prévues par son droit interne, qui doit assurer une protection adéquate des droits de l'homme et des libertés, en particulier des droits établis conformément aux obligations que celle-ci a souscrites en application de la Convention de sauvegarde des Droits de l'Homme et des Libertés fondamentales du Conseil de l'Europe (1950) et du Pacte international relatif aux droits civils et politiques des Nations Unies (1966), ou d'autres instruments internationaux applicables concernant les droits de l'homme, et qui doit intégrer le principe de la proportionnalité.

2 Lorsque cela est approprié, eu égard à la nature de la procédure ou du pouvoir concerné, ces conditions et sauvegardes incluent, entre autres, une supervision judiciaire ou d'autres formes de supervision indépendante, des motifs justifiant l'application ainsi que la limitation du champ d'application et de la durée du pouvoir ou de la procédure en question.

3 Dans la mesure où cela est conforme à l'intérêt public, en particulier à la bonne administration de la justice, chaque Partie examine l'effet des pouvoirs et procédures dans cette section sur les droits, responsabilités et intérêts légitimes des tiers.

Titre 2 – Conservation rapide de données informatiques stockées

Article 16 – Conservation rapide de données informatiques stockées

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour permettre à ses autorités compétentes d'ordonner ou d'imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification.

2 Lorsqu'une Partie fait application du paragraphe 1 ci-dessus, au moyen d'une injonction ordonnant à une personne de conserver des données stockées spécifiées se trouvant en sa possession ou sous son contrôle, cette Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger cette personne à conserver et à protéger l'intégrité desdites données pendant une durée aussi longue que nécessaire, au maximum de quatre-vingt-dix jours, afin de permettre aux autorités compétentes d'obtenir leur divulgation. Une Partie peut prévoir qu'une telle injonction soit renouvelée par la suite.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger le gardien des données ou une autre personne chargée de conserver celles-ci à garder le secret sur la mise en œuvre desdites procédures pendant la durée prévue par son droit interne.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 17 – Conservation et divulgation partielle rapides de données relatives au trafic

1 Afin d'assurer la conservation des données relatives au trafic, en application de l'article 16, chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires:

a pour veiller à la conservation rapide de ces données relatives au trafic, qu'un seul ou plusieurs fournisseurs de services aient participé à la transmission de cette communication; et

b pour assurer la divulgation rapide à l'autorité compétente de la Partie, ou à une personne désignée par cette autorité, d'une quantité suffisante de données relatives au trafic pour permettre l'identification par la Partie des fournisseurs de services et de la voie par laquelle la communication a été transmise.

2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Titre 3 – Injonction de produire

Article 18 – Injonction de produire

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner:

a à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un système informatique ou un support de stockage informatique; et

b à un fournisseur de services offrant des prestations sur le territoire de la Partie, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services.

2 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

3 Aux fins du présent article, l'expression «données relatives aux abonnés» désigne toute information, sous forme de données informatiques ou sous toute autre forme, détenue par un fournisseur de services et se rapportant aux abonnés de ses services, autres que des données relatives au trafic ou au contenu, et permettant d'établir:

a le type de service de communication utilisé, les dispositions techniques prises à cet égard et la période de service;

b l'identité, l'adresse postale ou géographique et le numéro de téléphone de l'abonné, et tout autre numéro d'accès, les données concernant la facturation et le paiement, disponibles sur la base d'un contrat ou d'un arrangement de services;

c toute autre information relative à l'endroit où se trouvent les équipements de communication, disponible sur la base d'un contrat ou d'un arrangement de services.

Titre 4 – Perquisition et saisie de données informatiques stockées

Article 19 – Perquisition et saisie de données informatiques stockées

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à perquisitionner ou à accéder d'une façon similaire :

a à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et

b à un support du stockage informatique permettant de stocker des données informatiques sur son territoire.

2 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour veiller à ce que, lorsque ses autorités perquisitionnent ou accèdent d'une façon similaire à un système informatique spécifique ou à une partie de celui-ci, conformément au paragraphe 1.a, et ont des raisons de penser que les données recherchées sont stockées dans un autre système informatique ou dans une partie de celui-ci situé sur son territoire, et que ces données sont légalement accessibles à partir du système initial ou disponibles pour ce système initial, lesdites autorités soient en mesure d'étendre rapidement la perquisition ou l'accès d'une façon similaire à l'autre système.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé en application des paragraphes 1 ou 2. Ces mesures incluent les prérogatives suivantes :

a saisir ou obtenir d'une façon similaire un système informatique ou une partie de celui-ci, ou un support de stockage informatique ;

b réaliser et conserver une copie de ces données informatiques ;

c préserver l'intégrité des données informatiques stockées pertinentes ;

d rendre inaccessibles ou enlever ces données informatiques du système informatique consulté.

4 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes à ordonner à toute personne connaissant le fonctionnement du système informatique ou les mesures appliquées pour protéger les données informatiques qu'il contient de fournir toutes les informations raisonnablement nécessaires, pour permettre l'application des mesures visées par les paragraphes 1 et 2.

5 Les pouvoirs et procédures mentionnés dans cet article doivent être soumis aux articles 14 et 15.

Titre 5 – Collecte en temps réel de données informatiques

Article 20 – Collecte en temps réel des données relatives au trafic

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes :

a à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire, et

b à obliger un fournisseur de services, dans le cadre de ses capacités techniques existantes :

i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique.

2 Lorsqu'une Partie, en raison des principes établis de son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place, adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au trafic associées à des communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté ainsi que toute information à ce sujet.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Article 21 – Interception de données relatives au contenu

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes en ce qui concerne un éventail d'infractions graves à définir en droit interne :

a à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, et

b à obliger un fournisseur de services, dans le cadre de ses capacités techniques :

i à collecter ou à enregistrer par l'application de moyens techniques existant sur son territoire, ou

ii à prêter aux autorités compétentes son concours et son assistance pour collecter ou enregistrer,

en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique.

2 Lorsqu'une Partie, en raison des principes établis dans son ordre juridique interne, ne peut adopter les mesures énoncées au paragraphe 1.a, elle peut à la place adopter les mesures législatives et autres qui se révèlent nécessaires pour assurer la collecte ou l'enregistrement en temps réel des données relatives au contenu de communications spécifiques transmises sur son territoire par l'application de moyens techniques existant sur ce territoire.

3 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour obliger un fournisseur de services à garder secrets le fait que l'un quelconque des pouvoirs prévus dans le présent article a été exécuté, ainsi que toute information à ce sujet.

4 Les pouvoirs et procédures mentionnés dans le présent article doivent être soumis aux articles 14 et 15.

Section 3 – Compétence

Article 22 – Compétence

1 Chaque Partie adopte les mesures législatives et autres qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction pénale établie conformément aux articles 2 à 11 de la présente Convention, lorsque l'infraction est commise :

a sur son territoire ; ou

b à bord d'un navire battant pavillon de cette Partie ; ou

c à bord d'un aéronef immatriculé selon les lois de cette Partie ; ou

d par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun Etat.

2 Chaque Partie peut se réserver le droit de ne pas appliquer, ou de n'appliquer que dans des cas ou des conditions spécifiques, les règles de compétence définies aux paragraphes 1.b à 1.d du présent article ou dans une partie quelconque de ces paragraphes.

3 Chaque Partie adopte les mesures qui se révèlent nécessaires pour établir sa compétence à l'égard de toute infraction mentionnée à l'article 24, paragraphe 1, de la présente Convention, lorsque l'auteur présumé de l'infraction est présent sur son territoire et ne peut être extradé vers une autre Partie au seul titre de sa nationalité, après une demande d'extradition.

4 La présente Convention n'exclut aucune compétence pénale exercée par une Partie conformément à son droit interne.

5 Lorsque plusieurs Parties revendiquent une compétence à l'égard d'une infraction présumée visée dans la présente Convention, les Parties concernées se concertent, lorsque cela est opportun, afin de déterminer la mieux à même d'exercer les poursuites.

Chapitre III – Coopération internationale

Section 1 – Principes généraux

Titre 1 – Principes généraux relatifs à la coopération internationale

Article 23 – Principes généraux relatifs à la coopération internationale

Les Parties coopèrent les unes avec les autres, conformément aux dispositions du présent chapitre, en application des instruments internationaux pertinents sur la coopération internationale en matière pénale, des arrangements reposant sur des législations uniformes ou réciproques et de leur droit national, dans la mesure la plus large possible, aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et des données informatiques ou pour recueillir les preuves, sous forme électronique, d'une infraction pénale.

Titre 2 – Principes relatifs à l'extradition

Article 24 – Extradition

1 a Le présent article s'applique à l'extradition entre les Parties pour les infractions pénales définies conformément aux articles 2 à 11 de la présente Convention, à condition qu'elles soient punissables dans la législation des deux Parties concernées par une peine privative de liberté pour une période maximale d'au moins un an, ou par une peine plus sévère.

b Lorsqu'il est exigé une peine minimale différente, sur la base d'un traité d'extradition tel qu'applicable entre deux ou plusieurs parties, y compris la Convention européenne d'extradition (STE n° 24), ou d'un arrangement reposant sur des législations uniformes ou réciproques, la peine minimale prévue par ce traité ou cet arrangement s'applique.

2 Les infractions pénales décrites au paragraphe 1 du présent article sont considérées comme incluses en tant qu'infractions pouvant donner lieu à extradition dans tout traité d'extradition existant entre ou parmi les Parties. Les Parties s'engagent à inclure de telles infractions comme infractions pouvant donner lieu à extradition dans tout traité d'extradition pouvant être conclu entre ou parmi elles.

3 Lorsqu'une Partie conditionne l'extradition à l'existence d'un traité et reçoit une demande d'extradition d'une autre Partie avec laquelle elle n'a pas conclu de traité d'extradition, elle peut considérer la présente Convention comme fondement juridique pour l'extradition au regard de toute infraction pénale mentionnée au paragraphe 1 du présent article.

4 Les Parties qui ne conditionnent pas l'extradition à l'existence d'un traité reconnaissent les infractions pénales mentionnées au paragraphe 1 du présent article comme des infractions pouvant donner lieu entre elles à l'extradition.

5 L'extradition est soumise aux conditions prévues par le droit interne de la Partie requise ou par les traités d'extradition en vigueur, y compris les motifs pour lesquels la Partie requise peut refuser l'extradition.

6 Si l'extradition pour une infraction pénale mentionnée au paragraphe 1 du présent article est refusée uniquement sur la base de la nationalité de la personne recherchée ou parce que la Partie requise s'estime compétente pour cette infraction, la Partie requise soumet l'affaire, à la demande de la Partie requérante, à ses autorités compétentes aux fins de poursuites, et rendra compte, en temps utile, de l'issue de l'affaire à la Partie requérante. Les autorités en question prendront leur décision et mèneront l'enquête et la procédure de la même manière que pour toute autre infraction de nature comparable, conformément à la législation de cette Partie.

7 a Chaque Partie communique au Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, le nom et l'adresse de chaque autorité responsable de l'envoi ou de la réception d'une demande d'extradition ou d'arrestation provisoire, en l'absence de traité.

b Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités ainsi désignées par les Parties. Chaque Partie doit veiller en permanence à l'exactitude des données figurant dans le registre.

Titre 3 – Principes généraux relatifs à l'entraide

Article 25 – Principes généraux relatifs à l'entraide

1 Les Parties s'accordent l'entraide la plus large possible aux fins d'investigations ou de procédures concernant les infractions pénales liées à des systèmes et à des données informatiques, ou afin de recueillir les preuves sous forme électronique d'une infraction pénale.

2 Chaque Partie adopte également les mesures législatives et autres qui se révèlent nécessaires pour s'acquitter des obligations énoncées aux articles 27 à 35.

3 Chaque Partie peut, en cas d'urgence, formuler une demande d'entraide ou les communications s'y rapportant par des moyens rapides de communication, tels que la télécopie ou le courrier

électronique, pour autant que ces moyens offrent des conditions suffisantes de sécurité et d'authentification (y compris, si nécessaire, le cryptage), avec confirmation officielle ultérieure si l'Etat requis l'exige. L'Etat requis accepte la demande et y répond par n'importe lequel de ces moyens rapides de communication.

4 Sauf disposition contraire expressément prévue dans les articles du présent chapitre, l'entraide est soumise aux conditions fixées par le droit interne de la Partie requise ou par les traités d'entraide applicables, y compris les motifs sur la base desquels la Partie requise peut refuser la coopération. La Partie requise ne doit pas exercer son droit de refuser l'entraide concernant les infractions visées aux articles 2 à 11 au seul motif que la demande porte sur une infraction qu'elle considère comme de nature fiscale.

5 Lorsque, conformément aux dispositions du présent chapitre, la Partie requise est autorisée à subordonner l'entraide à l'existence d'une double incrimination, cette condition sera considérée comme satisfaite si le comportement constituant l'infraction, pour laquelle l'entraide est requise, est qualifié d'infraction pénale par son droit interne, que le droit interne classe ou non l'infraction dans la même catégorie d'infractions ou qu'il la désigne ou non par la même terminologie que le droit de la Partie requérante.

Article 26 – Information spontanée

1 Une Partie peut, dans les limites de son droit interne et en l'absence de demande préalable, communiquer à une autre Partie des informations obtenues dans le cadre de ses propres enquêtes lorsqu'elle estime que cela pourrait aider la Partie destinataire à engager ou à mener à bien des enquêtes ou des procédures au sujet d'infractions pénales établies conformément à la présente Convention, ou lorsque ces informations pourraient aboutir à une demande de coopération formulée par cette Partie au titre du présent chapitre.

2 Avant de communiquer de telles informations, la Partie qui les fournit peut demander qu'elles restent confidentielles ou qu'elles ne soient utilisées qu'à certaines conditions. Si la Partie destinataire ne peut faire droit à cette demande, elle doit en informer l'autre Partie, qui devra alors déterminer si les informations en question devraient néanmoins être fournies. Si la Partie destinataire accepte les informations aux conditions prescrites, elle sera liée par ces dernières.

Titre 4 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

Article 27 – Procédures relatives aux demandes d'entraide en l'absence d'accords internationaux applicables

1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions des paragraphes 2 à 9 du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du reste de cet article.

2 a Chaque Partie désigne une ou plusieurs autorités centrales chargées d'envoyer les demandes d'entraide ou d'y répondre, de les exécuter ou de les transmettre aux autorités compétentes pour leur exécution ;

b Les autorités centrales communiquent directement les unes avec les autres ;

c Chaque Partie, au moment de la signature ou du dépôt de ses instruments de ratification, d'acceptation, d'approbation ou d'adhésion, communique au Secrétaire Général du Conseil de l'Europe les noms et adresses des autorités désignées en application du présent paragraphe ;

d Le Secrétaire Général du Conseil de l'Europe établit et tient à jour un registre des autorités centrales désignées par les Parties. Chaque Partie veille en permanence à l'exactitude des données figurant dans le registre.

3 Les demandes d'entraide sous le présent article sont exécutées conformément à la procédure spécifiée par la Partie requérante, sauf lorsqu'elle est incompatible avec la législation de la Partie requise.

4 Outre les conditions ou les motifs de refus prévus à l'article 25, paragraphe 4, l'entraide peut être refusée par la Partie requise :

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

5 La Partie requise peut surseoir à l'exécution de la demande si cela risquerait de porter préjudice à des enquêtes ou procédures conduites par ses autorités.

6 Avant de refuser ou de différer sa coopération, la Partie requise examine, après avoir le cas échéant consulté la Partie requérante, s'il peut être fait droit à la demande partiellement, ou sous réserve des conditions qu'elle juge nécessaires.

7 La Partie requise informe rapidement la Partie requérante de la suite qu'elle entend donner à la demande d'entraide. Elle doit motiver son éventuel refus d'y faire droit ou l'éventuel ajournement de la demande. La Partie requise informe également la Partie requérante de tout motif rendant l'exécution de l'entraide impossible ou étant susceptible de la retarder de manière significative.

8 La Partie requérante peut demander que la Partie requise garde confidentiels le fait et l'objet de toute demande formulée au titre du présent chapitre, sauf dans la mesure nécessaire à l'exécution de ladite demande. Si la Partie requise ne peut faire droit à cette demande de confidentialité, elle doit en informer rapidement la Partie requérante, qui devra alors déterminer si la demande doit néanmoins être exécutée.

9 a En cas d'urgence, les autorités judiciaires de la Partie requérante peuvent adresser directement à leurs homologues de la Partie requise les demandes d'entraide ou les communications s'y rapportant. Dans un tel cas, copie est adressée simultanément aux autorités centrales de la Partie requise par le biais de l'autorité centrale de la Partie requérante.

b Toute demande ou communication formulée au titre du présent paragraphe peut l'être par l'intermédiaire de l'Organisation internationale de police criminelle (Interpol).

c Lorsqu'une demande a été formulée en application de l'alinéa a. du présent article et lorsque l'autorité n'est pas compétente pour la traiter, elle la transmet à l'autorité nationale compétente et en informe directement la Partie requérante.

d Les demandes ou communications effectuées en application du présent paragraphe qui ne supposent pas de mesure de coercition peuvent être directement transmises par les autorités compétentes de la Partie requérante aux autorités compétentes de la Partie requise.

e Chaque Partie peut informer le Secrétaire Général du Conseil de l'Europe, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, que, pour des raisons d'efficacité, les demandes faites sous ce paragraphe devront être adressées à son autorité centrale.

Article 28 – Confidentialité et restriction d'utilisation

1 En l'absence de traité d'entraide ou d'arrangement reposant sur des législations uniformes ou réciproques en vigueur entre la Partie requérante et la Partie requise, les dispositions du présent article s'appliquent. Elles ne s'appliquent pas lorsqu'un traité, un arrangement ou une législation de ce type existent, à moins que les Parties concernées ne décident d'appliquer à la place tout ou partie du présent article.

2 La Partie requise peut subordonner la communication d'informations ou de matériels en réponse à une demande :

a à la condition que ceux-ci restent confidentiels lorsque la demande d'entraide ne pourrait être respectée en l'absence de cette condition ; ou

b à la condition qu'ils ne soient pas utilisés aux fins d'enquêtes ou de procédures autres que celles indiquées dans la demande.

3 Si la Partie requérante ne peut satisfaire à l'une des conditions énoncées au paragraphe 2, elle en informe rapidement la Partie requise, qui détermine alors si l'information doit néanmoins être fournie. Si la Partie requérante accepte cette condition, elle sera liée par celle-ci.

4 Toute Partie qui fournit des informations ou du matériel soumis à l'une des conditions énoncées au paragraphe 2 peut exiger de l'autre Partie qu'elle lui communique des précisions, en relation avec cette condition, quant à l'usage fait de ces informations ou de ce matériel.

Section 2 – Dispositions spécifiques

Titre 1 – Entraide en matière de mesures provisoires

Article 29 – Conservation rapide de données informatiques stockées

1 Une Partie peut demander à une autre Partie d'ordonner ou d'imposer d'une autre façon la conservation rapide de données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, et au sujet desquelles la Partie requérante a l'intention de soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation desdites données.

2 Une demande de conservation faite en application du paragraphe 1 doit préciser :

a l'autorité qui demande la conservation ;

b l'infraction faisant l'objet de l'enquête ou de procédures pénales et un bref exposé des faits qui s'y rattachent ;

c les données informatiques stockées à conserver et la nature de leur lien avec l'infraction ;

d toutes les informations disponibles permettant d'identifier le gardien des données informatiques stockées ou l'emplacement du système informatique ;

e la nécessité de la mesure de conservation ; et

f le fait que la Partie entend soumettre une demande d'entraide en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données informatiques stockées.

3 Après avoir reçu la demande d'une autre Partie, la Partie requise doit prendre toutes les mesures appropriées afin de procéder sans délai à la conservation des données spécifiées, conformément à son droit interne. Pour pouvoir répondre à une telle demande, la double incrimination n'est pas requise comme condition préalable à la conservation.

4 Une Partie qui exige la double incrimination comme condition pour répondre à une demande d'entraide visant la perquisition ou l'accès similaire, la saisie ou l'obtention par un moyen similaire ou la divulgation des données stockées peut, pour des infractions autres que celles établies conformément aux articles 2 à 11 de la présente Convention, se réserver le droit de refuser la demande de conservation au titre du présent article dans le cas où elle a des raisons de penser que, au moment de la divulgation, la condition de double incrimination ne pourra pas être remplie.

5 En outre, une demande de conservation peut être refusée uniquement :

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

b si la Partie requise estime que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à l'ordre public ou à d'autres intérêts essentiels.

6 Lorsque la Partie requise estime que la conservation simple ne suffira pas à garantir la disponibilité future des données, ou compromettra la confidentialité de l'enquête de la Partie requérante, ou nuira d'une autre façon à celle-ci, elle en informe rapidement la Partie requérante, qui décide alors s'il convient néanmoins d'exécuter la demande.

7 Toute conservation effectuée en réponse à une demande visée au paragraphe 1 sera valable pour une période d'au moins soixante jours afin de permettre à la Partie requérante de soumettre une demande en vue de la perquisition ou de l'accès par un moyen similaire, de la saisie ou de l'obtention par un moyen similaire, ou de la divulgation des données. Après la réception d'une telle demande, les données doivent continuer à être conservées en attendant l'adoption d'une décision concernant la demande.

Article 30 – Divulgation rapide de données conservées

1 Lorsque, en exécutant une demande de conservation de données relatives au trafic concernant une communication spécifique formulée en application de l'article 29, la Partie requise découvre qu'un fournisseur de services dans un autre Etat a participé à la transmission de cette communication, la Partie requise divulgue rapidement à la Partie requérante une quantité suffisante de données concernant le trafic, aux fins d'identifier ce fournisseur de services et la voie par laquelle la communication a été transmise.

2 La divulgation de données relatives au trafic en application du paragraphe 1 peut être refusée seulement :

a si la demande porte sur une infraction que la Partie requise considère comme étant de nature politique ou liée à une infraction de nature politique ; ou

b si elle considère que le fait d'accéder à la demande risquerait de porter atteinte à sa souveraineté, à sa sécurité, à son ordre public ou à d'autres intérêts essentiels.

Titre 2 – Entraide concernant les pouvoirs d'investigation

Article 31 – Entraide concernant l'accès aux données stockées

1 Une Partie peut demander à une autre Partie de perquisitionner ou d'accéder de façon similaire, de saisir ou d'obtenir de façon similaire, de divulguer des données stockées au moyen d'un système informatique se trouvant sur le territoire de cette autre Partie, y compris les données conservées conformément à l'article 29.

2 La Partie requise satisfait à la demande en appliquant les instruments internationaux, les arrangements et les législations mentionnés à l'article 23, et en se conformant aux dispositions pertinentes du présent chapitre.

3 La demande doit être satisfaite aussi rapidement que possible dans les cas suivants :

a il y a des raisons de penser que les données pertinentes sont particulièrement sensibles aux risques de perte ou de modification ; ou

b les instruments, arrangements et législations visés au paragraphe 2 prévoient une coopération rapide.

Article 32 – Accès transfrontière à des données stockées, avec consentement ou lorsqu'elles sont accessibles au public

Une Partie peut, sans l'autorisation d'une autre Partie :

a accéder à des données informatiques stockées accessibles au public (source ouverte), quelle que soit la localisation géographique de ces données ; ou

b accéder à, ou recevoir au moyen d'un système informatique situé sur son territoire, des données informatiques stockées situées dans un autre Etat, si la Partie obtient le consentement légal et volontaire de la personne légalement autorisée à lui divulguer ces données au moyen de ce système informatique.

Article 33 – Entraide dans la collecte en temps réel de données relatives au trafic

1 Les Parties s'accordent l'entraide dans la collecte en temps réel de données relatives au trafic, associées à des communications spécifiées sur leur territoire, transmises au moyen d'un système informatique. Sous réserve des dispositions du paragraphe 2, cette entraide est régie par les conditions et les procédures prévues en droit interne.

2 Chaque Partie accorde cette entraide au moins à l'égard des infractions pénales pour lesquelles la collecte en temps réel de données concernant le trafic serait disponible dans une affaire analogue au niveau interne.

Article 34 – Entraide en matière d'interception de données relatives au contenu

Les Parties s'accordent l'entraide, dans la mesure permise par leurs traités et lois internes applicables, pour la collecte ou l'enregistrement en temps réel de données relatives au contenu de communications spécifiques transmises au moyen d'un système informatique.

Titre 3 – Réseau 24/7

Article 35 – Réseau 24/7

1 Chaque Partie désigne un point de contact joignable vingt-quatre heures sur vingt-quatre, sept jours sur sept, afin d'assurer une assistance immédiate pour des investigations concernant

les infractions pénales liées à des systèmes et à des données informatiques, ou pour recueillir les preuves sous forme électronique d'une infraction pénale. Cette assistance englobera la facilitation, ou, si le droit et la pratique internes le permettent, l'application directe des mesures suivantes:

a apport de conseils techniques;

b conservation des données, conformément aux articles 29 et 30;

c recueil de preuves, apport d'informations à caractère juridique, et localisation des suspects.

2 a Le point de contact d'une Partie aura les moyens de correspondre avec le point de contact d'une autre Partie selon une procédure accélérée.

b Si le point de contact désigné par une Partie ne dépend pas de l'autorité ou des autorités de cette Partie responsables de l'entraide internationale ou de l'extradition, le point de contact veillera à pouvoir agir en coordination avec cette ou ces autorités, selon une procédure accélérée.

3 Chaque Partie fera en sorte de disposer d'un personnel formé et équipé en vue de faciliter le fonctionnement du réseau.

Chapitre IV – Clauses finales

Article 36 – Signature et entrée en vigueur

1 La présente Convention est ouverte à la signature des Etats membres du Conseil de l'Europe et des Etats non membres qui ont participé à son élaboration.

2 La présente Convention est soumise à ratification, acceptation ou approbation. Les instruments de ratification, d'acceptation ou d'approbation sont déposés près le Secrétaire Général du Conseil de l'Europe.

3 La présente Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date à laquelle cinq Etats, incluant au moins trois Etats membres du Conseil de l'Europe, auront exprimé leur consentement à être liés par la Convention, conformément aux dispositions des paragraphes 1 et 2.

4 Pour tout Etat signataire qui exprimera ultérieurement son consentement à être lié par la Convention, celle-ci entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de l'expression de son consentement à être lié par la Convention, conformément aux dispositions des paragraphes 1 et 2.

Article 37 – Adhésion à la Convention

1 Après l'entrée en vigueur de la présente Convention, le Comité des Ministres du Conseil de l'Europe peut, après avoir consulté les Etats contractants à la Convention et en avoir obtenu l'assentiment unanime, inviter tout Etat non membre du Conseil, n'ayant pas participé à son élaboration, à adhérer à la présente Convention. La décision est prise à la majorité prévue à l'article 20.d du Statut du Conseil de l'Europe et à l'unanimité des représentants des Etats contractants ayant le droit de siéger au Comité des Ministres.

2 Pour tout Etat adhérent à la Convention, conformément au paragraphe 1 ci-dessus, la Convention entrera en vigueur le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de dépôt de l'instrument d'adhésion près le Secrétaire Général du Conseil de l'Europe.

Article 38 – Application territoriale

1 Tout Etat peut, au moment de la signature ou au moment du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, désigner le ou les territoires auxquels s'appliquera la présente Convention.

2 Tout Etat peut, à tout autre moment par la suite, par déclaration adressée au Secrétaire Général du Conseil de l'Europe, étendre l'application de la présente Convention à tout autre territoire désigné dans la déclaration. La Convention entrera en vigueur à l'égard de ce territoire le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la déclaration par le Secrétaire Général.

3 Toute déclaration faite en application des deux paragraphes précédents peut être retirée, en ce qui concerne tout territoire désigné dans cette déclaration, par notification adressée au Secrétaire Général du Conseil de l'Europe. Le retrait prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de ladite notification par le Secrétaire Général.

Article 39 – Effets de la Convention

1 L'objet de la présente Convention est de compléter les traités ou les accords multilatéraux ou bilatéraux applicables existant entre les Parties, y compris les dispositions :

- de la Convention européenne d'extradition, ouverte à la signature le 13 décembre 1957, à Paris (STE n° 24) ;
- de la Convention européenne d'entraide judiciaire en matière pénale, ouverte à la signature le 20 avril 1959, à Strasbourg (STE n° 30) ;
- du Protocole additionnel à la Convention européenne d'entraide judiciaire en matière pénale, ouvert à la signature le 17 mars 1978, à Strasbourg (STE n° 99).

2 Si deux ou plusieurs Parties ont déjà conclu un accord ou un traité relatif aux matières traitées par la présente Convention, ou si elles ont autrement établi leurs relations sur ces sujets, ou si elles le feront à l'avenir, elles ont aussi la faculté d'appliquer ledit accord ou traité ou d'établir leurs relations en conséquence, au lieu de la présente Convention. Toutefois, lorsque les Parties établiront leurs relations relatives aux matières faisant l'objet de la présente Convention d'une manière différente de celle y prévue, elles le feront d'une manière qui ne soit pas incompatible avec les objectifs et les principes de la Convention.

3 Rien dans la présente Convention n'affecte d'autres droits, restrictions, obligations et responsabilités d'une Partie.

Article 40 – Déclarations

Par déclaration écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la faculté d'exiger, le cas échéant, un ou plusieurs éléments supplémentaires tels que prévus aux articles 2, 3, 6, paragraphe 1.b, 7, 9, paragraphe 3, et 27, paragraphe 9.e.

Article 41 – Clause fédérale

1 Un Etat fédéral peut se réserver le droit d'honorer les obligations contenues dans le chapitre II de la présente Convention dans la mesure où celles-ci sont compatibles avec les principes fondamentaux qui gouvernent les relations entre son gouvernement central et les Etats constituants ou autres entités territoriales analogues, à condition qu'il soit en mesure de coopérer sur la base du chapitre III.

2 Lorsqu'il fait une réserve prévue au paragraphe 1, un Etat fédéral ne saurait faire usage des termes d'une telle réserve pour exclure ou diminuer de manière substantielle ses obligations en vertu du chapitre II. En tout état de cause, il se dote de moyens étendus et effectifs permettant la mise en oeuvre des mesures prévues par ledit chapitre.

3 En ce qui concerne les dispositions de cette Convention dont l'application relève de la compétence législative de chacun des Etats constituants ou autres entités territoriales analogues, qui ne sont pas, en vertu du système constitutionnel de la fédération, tenus de prendre des mesures législatives, le gouvernement fédéral porte, avec son avis favorable, lesdites dispositions à la connaissance des autorités compétentes des Etats constituants, en les encourageant à adopter les mesures appropriées pour les mettre en œuvre.

Article 42 – Réserves

Par notification écrite adressée au Secrétaire Général du Conseil de l'Europe, tout Etat peut, au moment de la signature ou du dépôt de son instrument de ratification, d'acceptation, d'approbation ou d'adhésion, déclarer qu'il se prévaut de la ou les réserves prévues à l'article 4, paragraphe 2, à l'article 6, paragraphe 3, à l'article 9, paragraphe 4, à l'article 10, paragraphe 3, à l'article 11, paragraphe 3, à l'article 14, paragraphe 3, à l'article 22, paragraphe 2, à l'article 29, paragraphe 4, et à l'article 41, paragraphe 1. Aucune autre réserve ne peut être faite.

Article 43 – Statut et retrait des réserves

1 Une Partie qui a fait une réserve conformément à l'article 42 peut la retirer en totalité ou en partie par notification adressée au Secrétaire Général du Conseil de l'Europe. Ce retrait prend effet à la date de réception de ladite notification par le Secrétaire Général. Si la notification indique que le retrait d'une réserve doit prendre effet à une date précise, et si cette date est postérieure à celle à laquelle le Secrétaire Général reçoit la notification, le retrait prend effet à cette date ultérieure.

2 Une Partie qui a fait une réserve comme celles mentionnées à l'article 42 retire cette réserve, en totalité ou en partie, dès que les circonstances le permettent.

3 Le Secrétaire Général du Conseil de l'Europe peut périodiquement demander aux Parties ayant fait une ou plusieurs réserves comme celles mentionnées à l'article 42 des informations sur les perspectives de leur retrait.

Article 44 – Amendements

1 Des amendements à la présente Convention peuvent être proposés par chaque Partie, et sont communiqués par le Secrétaire Général du Conseil de l'Europe aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer, conformément aux dispositions de l'article 37.

2 Tout amendement proposé par une Partie est communiqué au Comité européen pour les problèmes criminels (CDPC), qui soumet au Comité des Ministres son avis sur ledit amendement.

3 Le Comité des Ministres examine l'amendement proposé et l'avis soumis par le CDPC et, après consultation avec les Etats non membres parties à la présente Convention, peut adopter l'amendement.

4 Le texte de tout amendement adopté par le Comité des Ministres conformément au paragraphe 3 du présent article est communiqué aux Parties pour acceptation.

5 Tout amendement adopté conformément au paragraphe 3 du présent article entre en vigueur le trentième jour après que toutes les Parties ont informé le Secrétaire Général de leur acceptation.

Article 45 – Règlement des différends

1 Le Comité européen pour les problèmes criminels du Conseil de l'Europe (CDPC) est tenu informé de l'interprétation et de l'application de la présente Convention.

2 En cas de différend entre les Parties sur l'interprétation ou l'application de la présente Convention, les Parties s'efforceront de parvenir à un règlement du différend par la négociation ou par tout autre moyen pacifique de leur choix, y compris la soumission du différend au CDPC, à un tribunal arbitral qui prendra des décisions qui lieront les Parties au différend, ou à la Cour internationale de justice, selon un accord entre les Parties concernées.

Article 46 – Concertation des Parties

1 Les Parties se concertent périodiquement, au besoin, afin de faciliter :

a l'usage et la mise en œuvre effectifs de la présente Convention, y compris l'identification de tout problème en la matière, ainsi que les effets de toute déclaration ou réserve faite conformément à la présente Convention ;

b l'échange d'informations sur les nouveautés juridiques, politiques ou techniques importantes observées dans le domaine de la criminalité informatique et la collecte de preuves sous forme électronique ;

c l'examen de l'éventualité de compléter ou d'amender la Convention.

2 Le Comité européen pour les problèmes criminels (CDPC) est tenu périodiquement au courant du résultat des concertations mentionnées au paragraphe 1.

3 Le CDPC facilite, au besoin, les concertations mentionnées au paragraphe 1 et adopte les mesures nécessaires pour aider les Parties dans leurs efforts visant à compléter ou amender la Convention. Au plus tard à l'issue d'un délai de trois ans à compter de l'entrée en vigueur de la présente Convention, le CDPC procédera, en coopération avec les Parties, à un réexamen de l'ensemble des dispositions de la Convention et proposera, le cas échéant, les amendements appropriés.

4 Sauf lorsque le Conseil de l'Europe les prend en charge, les frais occasionnés par l'application des dispositions du paragraphe 1 sont supportés par les Parties, de la manière qu'elles déterminent.

5 Les Parties sont assistées par le Secrétariat du Conseil de l'Europe dans l'exercice de leurs fonctions découlant du présent article.

Article 47 – Dénonciation

1 Toute Partie peut, à tout moment, dénoncer la présente Convention par notification au Secrétaire Général du Conseil de l'Europe.

2 La dénonciation prendra effet le premier jour du mois qui suit l'expiration d'une période de trois mois après la date de réception de la notification par le Secrétaire Général.

Article 48 – Notification

Le Secrétaire Général du Conseil de l'Europe notifie aux Etats membres du Conseil de l'Europe, aux Etats non membres ayant pris part à l'élaboration de la présente Convention, ainsi qu'à tout Etat y ayant adhéré ou ayant été invité à y adhérer :

a toute signature ;

b le dépôt de tout instrument de ratification, d'acceptation, d'approbation ou d'adhésion ;

c toute date d'entrée en vigueur de la présente Convention, conformément à ses articles 36 et 37 ;

d toute déclaration faite en application de l'article 40 ou toute réserve faite en application de l'article 42 ;

e tout autre acte, notification ou communication ayant trait à la présente Convention.

In witness whereof the undersigned, being duly authorised thereto, have signed this Convention.

Done at Budapest, this 23rd day of November 2001, in English and in French, both texts being equally authentic, in a single copy which shall be deposited in the archives of the Council of Europe. The Secretary General of the Council of Europe shall transmit certified copies to each member State of the Council of Europe, to the non-member States which have participated in the elaboration of this Convention, and to any State invited to accede to it.

En foi de quoi, les soussignés, dûment autorisés à cet effet, ont signé la présente Convention.

Fait à Budapest, le 23 novembre 2001, en français et en anglais, les deux textes faisant également foi, en un seul exemplaire qui sera déposé dans les archives du Conseil de l'Europe. Le Secrétaire Général du Conseil de l'Europe en communiquera copie certifiée conforme à chacun des Etats membres du Conseil de l'Europe, aux Etats non membres qui ont participé à l'élaboration de la Convention et à tout Etat invité à y adhérer.

Certified a true copy of the sole original document, in English and in French, deposited in the archives of the Council of Europe.

Copie certifiée conforme à l'exemplaire original unique en langues française et anglaise, déposé dans les archives du Conseil de l'Europe.

Strasbourg, 13 janvier 2002

The Director General of Legal Affairs of the Council of Europe,

Le Directeur Général des Affaires Juridiques du Conseil de l'Europe,

Guy DEVEL

CONVENZIONE DEL CONSIGLIO D'EUROPA SULLA CRIMINALITÀ INFORMATICA (*)

Budapest, 23.XI.2001

PREAMBOLO

GLI STATI MEMBRI DEL CONSIGLIO D'EUROPA E GLI ALTRI STATI FIRMATARI

considerando che lo scopo del Consiglio d'Europa è quello di ottenere un legame più stretto fra i propri membri;

riconoscendo l'interesse ad intensificare la collaborazione con gli altri Stati parte in questa Convenzione;

convinti della necessità di perseguire, come questione prioritaria, una politica comune in campo penale finalizzata alla protezione della società contro la criminalità informatica, adottando una legislazione appropriata e sviluppando la cooperazione internazionale;

consci dei profondi cambiamenti dipendenti dall'introduzione della tecnologia digitale, dalla convergenza e costante globalizzazione delle reti informatiche;

preoccupati dei rischi che le reti informatiche e le informazioni in formato elettronico possano anche essere utilizzate per commettere reati e che le prove connesse a tali reati possano essere conservate e trasferite tramite queste reti;

(*) Testo non ufficiale.

riconoscendo la necessità della cooperazione tra gli Stati e le società private nella lotta alla criminalità informatica e la necessità di tutelare gli interessi legittimi nell'uso e nello sviluppo delle tecnologie informatiche;

ritenendo che una lotta sostanziale alla criminalità informatica richiede una crescente, veloce e ben funzionante cooperazione internazionale in campo penale;

convinti che la presente Convenzione sia necessaria come deterrente per azioni dirette contro la segretezza, l'integrità e la disponibilità dei sistemi informatici, delle reti e dei dati informatici, così come per l'uso improprio di questi sistemi, reti ed informazioni, attraverso la criminalizzazione di questi comportamenti, come descritto nella presente Convenzione, e attraverso l'adozione di poteri sufficienti per combattere realmente questi reati, facilitando la loro individuazione, investigazione e l'esercizio dell'azione penale a livello sia nazionale che internazionale e prevedendo accordi per una cooperazione internazionale più veloce e affidabile;

tenendo presente la necessità di garantire un equo bilanciamento tra l'interesse per l'azione repressiva ed il rispetto dei diritti umani fondamentali come previsto nella Convenzione del Consiglio d'Europa del 1950 per la Tutela dei Diritti Umani e le Libertà Fondamentali, la Convenzione Internazionale delle Nazioni Unite del 1966 sui Diritti Civili e Politici e gli altri trattati applicabili sui diritti umani che riaffermano il diritto di ciascuno di avere opinioni senza condizionamenti, come anche il diritto alla libertà di espressione, incluso il diritto di cercare, ricevere, e trasmettere informazioni e idee di ogni tipo, senza limiti di frontiere, e il diritto al rispetto della *privacy*;

consapevoli anche del diritto alla tutela delle informazioni personali, ad esempio, in base alla Convenzione del 1981 del Consiglio d'Europa per la tutela degli Individui con riguardo alla gestione automatizzata dei dati personali;

tenuto conto della Convenzione delle Nazioni Unite del 1989 sui diritti dei minori e della Convenzione del 1999 dell'Organizzazione Internazionale del Lavoro sulle peggiori forme di lavoro minorile;

tenendo presente la Convenzione del Consiglio d'Europa sulla cooperazione in campo penale ed anche i trattati simili che esistono tra gli Stati membri del Consiglio d'Europa e gli altri Stati, e mettendo in evidenza che la presente Convenzione viene intesa come integrazione di queste convenzioni al fine di rendere più efficienti le indagini e l'azione penale su reati commessi in materia di sistemi informatici ed informazioni e consentire la raccolta di prove di un reato in forma elettronica;

accogliendo con favore i recenti sviluppi, quali la migliore conoscenza in campo internazionale e la cooperazione nella lotta alla criminalità informatica, inclusa l'azione intrapresa dalle Nazioni Unite, l'OECD, l'Unione Europea e il G8;

richiamando le Raccomandazioni del Comitato dei Ministri No. R (85) 10 riguardante la concreta applicazione della Convenzione Europea sulla Mutua Assistenza Legale in Campo Penale nel rispetto delle Rogatorie per l'intercettazione delle telecomunicazioni, No. R (88) 2 sulla pirateria nel campo del *copyright* e il diritto dei vicini, No. R (87) 15 che regola l'uso di informazioni personali da parte delle forze dell'ordine, No. R (95) 4 sulla protezione dei dati personali nell'area dei servizi delle telecomunicazioni, con particolare riguardo ai servizi telefonici, come anche la No. R (89) 9 sui crimini connessi all'uso di computer, prevedendo delle linee giuda per le legislazioni nazionali riguardanti la definizione di alcuni crimini informatici e No. R (95) 13 riguardante problemi di diritto procedurale penale collegati con l'*information technology*;

avendo riguardo alla Risoluzione No. 1 adottata dai Ministri della Giustizia Europei nel corso della loro 21° Conferenza (Praga, 10 e 11 Giugno 1997), che raccomandava che il Comitato dei Ministri supportasse il lavoro sulla criminalità informatica svolto dal Comitato Europeo sui Problemi Penali (CDPC) al fine di rendere le legislazioni dei singoli Paesi più simili tra loro e di consentire l'uso di sistemi pratici nelle indagini su questi reati, così come la Risoluzione No. 3 adottata alla 23° Conferenza dei Ministri Europei della Giustizia (Londra, 8 e 9 Giugno 2000) che incoraggia le parti a proseguire nei loro sforzi volti a trovare soluzioni adeguate per consentire al maggior numero di Stati di divenire parti della Convenzione e riconoscendo la necessità di un rapido ed efficiente sistema di cooperazione internazionale che prenda nel dovuto conto la richiesta specifica di lotta contro la criminalità informatica;
avendo anche riguardo al Piano d'Azione dei Capi di Stato e dei Governi del Consiglio d'Europa elaborato in occasione del loro Secondo Summit (Strasburgo, 10 e 11 Ottobre 1997) per cercare risposte comuni allo sviluppo delle nuove tecnologie basate su *standards* e valori propri del Consiglio d'Europa,

HANNO CONVENUTO QUANTO SEGUE

CAPITOLO I
USO DEI TERMINI

Articolo 1
Definizioni

Ai fini della presente Convenzione:

a. "*sistema informatico*" indica qualsiasi apparecchiatura o gruppo di apparecchiature interconnesse o collegate, una o più delle quali, in base ad un programma, compiono l'elaborazione automatica di dati;

b. "*dati informatici* " indica qualunque presentazione di fatti, informazioni o concetti in forma suscettibile di essere utilizzata in un sistema computerizzato, incluso un programma in grado di consentire ad un sistema computerizzato di svolgere una funzione;

c. "*service provider*" (fornitore di servizi), indica:

1. qualunque entità pubblica o privata che fornisce agli utenti dei propri servizi la possibilità di comunicare attraverso un sistema informatico;

2. qualunque altra entità che processa o archivia dati informatici per conto di tale servizio di comunicazione o per utenti di tale servizio;

d. "*trasmissione di dati*" indica qualsiasi informazione computerizzata relativa ad una comunicazione attraverso un sistema informatico che costituisce una parte nella catena di comunicazione, indicando l'origine della comunicazione, la destinazione, il percorso, il tempo, la data, la grandezza, la durata o il tipo del servizio.

CAPITOLO II
PROVVEDIMENTI DA ADOTTARE A LIVELLO NAZIONALE

SEZIONI I
DIRITTO PENALE SOSTANZIALE

TITOLO I
REATI CONTRO LA RISERVATEZZA, L'INTEGRITÀ E LA DISPONIBILITÀ DEI DATI E DEI SISTEMI INFORMATICI

Articolo 2
Accesso illegale ad un sistema informatico

Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per sanzionare come reato in base alla propria legge nazionale l'accesso all'intero sistema informatico o a parte di esso senza autorizzazione.

Una Parte può richiedere che il reato venga commesso violando misure di sicurezza con l'intenzione di ottenere informazioni all'interno di un computer o con altro intento illegale o in relazione ad un sistema informatico che è connesso ad un altro sistema informatico.

Articolo 3

Intercettazione abusiva

Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale l'intercettazione senza autorizzazione, fatta con strumenti tecnici, di trasmissioni non pubbliche di dati informatici a, da o all'interno di un sistema informatico, incluse le emissioni elettromagnetiche da un sistema informatico che ha tali dati informatici. Una Parte può richiedere che il reato venga commesso con intento illegale o in relazione ad un sistema informatico che è connesso ad un altro sistema informatico.

Articolo 4

Attentato all'integrità dei dati

1. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale il danneggiamento, la cancellazione, il deterioramento, la modifica o la soppressione di dati informatici senza autorizzazione.

2. Ogni Parte può riservarsi il diritto di richiedere che la condotta descritta nel paragrafo 1. sia di grave danno.

Articolo 5

Attentato all'integrità di in un sistema

Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale il serio impedimento, senza alcun diritto, del funzionamento di un sistema informatico tramite l'introduzione, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di dati informatici.

Articolo 6

Abuso di apparecchiature

1 Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commessi intenzionalmente e senza autorizzazione:

a. la fabbricazione, la vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione o l'utilizzabilità in altro modo di:

1. un'apparecchiatura, incluso un programma per computer, destinato o utilizzato principalmente al fine di commettere un qualsiasi reato in base agli articoli da 2 a 5 di cui sopra;

2. una *password* di un computer, un codice d'accesso, o informazioni simili con le quali l'intero sistema informatico o una sua parte sono accessibili, con l'intento di commettere qualsiasi reato in base agli articoli da 2 a 5 di cui sopra;

b. il possesso di uno elemento di cui ai sopra citati paragrafi a. 1. o 2., con l'intento di utilizzarlo allo scopo di commettere qualche reato in base agli articoli da 2 a 5. Una Parte può richiedere per legge che vi sia il possesso di un certo numero di tali elementi perché vi sia una responsabilità penale.

2. Questo articolo non va interpretato nel senso di prevedere una responsabilità penale laddove la produzione, la vendita, l'approvvigionamento per l'uso, l'importazione, la distribuzione o l'utilizzazione in altro modo o il possesso di cui al paragrafo 1. di questo articolo, non avvenga allo scopo di commettere un reato in base agli articoli da 2 a 5 di questa Convenzione, come anche per il collaudo autorizzato o la protezione di un sistema informatico.

3. Ogni Parte può riservarsi il diritto di non applicare il paragrafo 1. di questo articolo, purché tale riserva non concerna la vendita, la distribuzione o l'utilizzazione in altro modo degli elementi riferiti al paragrafo 1 a. 2. di questo articolo.

TITOLO II
REATI INFORMATICI

Articolo 7
Falsificazione informatica

Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commessi intenzionalmente e senza alcun diritto, l'introduzione, l'alterazione, il possesso o la soppressione di dati informatici derivanti da dati non autentici con l'intento che essi siano presi in considerazione o utilizzati con fini legali come se fossero autentici, senza avere riguardo al fatto che i dati siano o meno direttamente leggibili o intelligibili. Una Parte può richiedere che il reato venga commesso fraudolentemente, o con un intento illegale paragonabile, perché vi sia una responsabilità penale.

Articolo 8

Frode informatica

Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commesso intenzionalmente e senza alcun diritto, il cagionare un danno patrimoniale ad altra persona:

a. con ogni introduzione, alterazione, cancellazione o soppressione di dati informatici;

b. con ogni interferenza nel funzionamento di un sistema informatico, con l'intento fraudolento o illegale di procurare, senza alcun diritto, un beneficio economico per se stesso o altri.

TITOLO II
REATI RELATIVI AI CONTENUTI

Articolo 9

Reati relativi alla pornografia infantile

1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commesse intenzionalmente e senza alcun diritto:

a. la produzione di pornografia infantile allo scopo della sua diffusione attraverso un sistema informatico;

b. l'offerta o la messa a disposizione di pornografia infantile attraverso un sistema informatico;

c. la distribuzione o la trasmissione di pornografia infantile attraverso un sistema informatico;

d. il procurare pornografia infantile attraverso un sistema informatico per se stessi o altri;

e. il possesso di pornografia infantile attraverso un sistema informatico o uno strumento di archiviazione di dati informatici.

2. Ai fini del Paragrafo 1. di cui sopra, l'espressione " pornografia infantile " include il materiale pornografico che raffigura:

a. un minore coinvolto in un comportamento sessuale esplicito;

b. un soggetto che sembra essere un minore coinvolto in un comportamento sessuale esplicito;

c. immagini realistiche raffiguranti un minore coinvolto in un comportamento sessuale esplicito;

3. Ai fini del Paragrafo 2. di cui sopra, il termine "minore" include tutte le persone sotto i 18 anni di età. Una Parte può comunque richiedere un età minore, che non potrà essere inferiore ai 16 anni.

4. Ogni Parte può riservarsi il diritto di non applicare in tutto o in parte il paragrafo 1., sottoparagrafi d. ed e., e 2, sottoparagrafi b.e c.

TITOLO IV
REATI CONTRO LA PROPRIETÀ INTELLETTUALE E DIRITTI COLLEGATI

Articolo 10
Reati contro la proprietà intellettuale e diritti collegati

1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale la violazione della proprietà intellettuale, come definita in base alla legge di quella Parte, tenendo fede agli obblighi che ha assunto in base al *Paris Act* del 24 luglio 1971 che ha modificato la Convenzione di Berna sulla protezione delle opere letterarie e artistiche, l'Accordo sugli aspetti commerciali dei diritti sulla proprietà intellettuale e il Trattato OMPI sulla proprietà intellettuale, con l'eccezione di tutti i diritti morali conferiti da queste convenzioni, se tali atti sono commessi deliberatamente, su scala commerciale e attraverso l'utilizzo di un sistema informatico.

2. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale la violazione di diritti connessi come definiti dalla legge di quello Stato Parte, tenendo fede agli obblighi che ha assunto in base alla Convenzione Internazionale per la protezione degli artisti, interpreti ed esecutori, produttori di fonogrammi e organismi di radiodiffusione (Convenzione di Roma), all'Accordo sugli aspetti commerciali dei diritti sulla proprietà intellettuale e il Trattato OMPI sull'interpretazione e l'esecuzione e i fonogrammi, con l'eccezione di tutti i diritti morali conferiti da queste convenzioni, se tali atti sono commessi deliberatamente, su scala commerciale e attraverso l'utilizzo di un sistema informatico.

3. Una Parte può riservarsi il diritto di non imporre la responsabilità penale in base ai paragrafi 1. e 2. di questo articolo in determinate circostanze, a condizione che altri rimedi efficaci siano disponibili e che tale riserva non deroghi agli obblighi internazionalmente

assunti da questa Parte in applicazione degli strumenti internazionali menzionati nei paragrafi 1. e 2. di questo articolo.

TITOLO V
ALTRE FORME RESPONSABILITÀ E SANZIONI

Articolo 11
Tentativo e complicità

1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, ogni complicità quando sia commessa intenzionalmente in vista della perpetrazione di un'infrazione di cui agli articoli da 2 a 10 della presente Convenzione, con l'intento che tale reato venga commesso.

2. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire come reato in base alla propria legge nazionale, se commesso volontariamente, il tentativo di commettere ogni tipo di reato in base agli articoli da 3 a 5, 7,8,9.1 a. e c. della presente Convenzione.

3. Ogni parte può riservarsi il diritto di non applicare, in tutto o in parte, il paragrafo 2 di questo articolo.

Articolo 12
Responsabilità delle Persone Giuridiche

1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie affinché le persone giuridiche possano essere ritenute responsabili di un reato in base a questa Convenzione commesso per loro conto da una persona fisica che agisca sia individualmente che come membro di un organo di una persona giuridica che eserciti un potere di direzione al suo interno, nei termini che seguono:

a. un potere di rappresentanza della persona giuridica;
b. un'autorità per assumere decisioni nel nome della persona giuridica;
c. un'autorità per esercitare un controllo all'interno della persona giuridica.

2. In aggiunta ai casi già previsti nel paragrafo 1. di questo articolo, ogni Parte deve adottare le misure necessarie affinché una persona giuridica possa essere ritenuta responsabile se la mancanza di sorveglianza o controllo di una persona fisica di cui al paragrafo 1. ha reso possibile la commissione di reati previsti al paragrafo 1. per conto della persona giuridica da parte di una persona fisica che agisca sotto la sua autorità.

3. Secondo i principi giuridici della Parte, la responsabilità delle persone giuridiche può essere penale, civile o amministrativa.

4.Questa responsabilità è stabilita senza pregiudizio per la responsabilità penale delle persone fisiche che hanno commesso il reato.

Articolo 13

Sanzioni e Strumenti

1.Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie affinché i reati previsti in applicazione degli articoli da 2 a 11 possano essere puniti con sanzioni effettive, proporzionate e dissuasive, che includano la privazione della libertà.

2.Ogni parte deve assicurarsi che le persone giuridiche ritenute responsabili in base all'articolo 12 siano assoggettate a sanzioni penali o non penali effettive, proporzionate e dissuasive o ad altre misure, incluse sanzioni pecuniarie.

SEZIONE II
DIRITTO PROCEDURALE

TITOLO I
DISPOSIZIONI COMUNI

Articolo 14

Ambito di applicazione delle disposizioni procedurali

1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per definire i poteri e le procedure previste in questa Sezione per indagini o procedimenti penali specifici.

2. Salvo contraria disposizione risultante all'articolo 21, ogni Parte deve applicare i poteri e le procedure menzionati nel paragrafo 1.:

a. ai reati previsti in conformità agli articoli da 2 a 11 della presente Convenzione;

b. a tutti gli altri reati commessi attraverso un sistema informatico;

c. all'insieme delle prove elettroniche di un reato.

3. a. Ogni Parte si può riservare il diritto di applicare le misure di cui all'articolo 20 solamente ai reati o alle categorie di reati specificati nella riserva, purché l'ambito di tali reati o categorie di reato non sia più ristretto di quello dei reati ai quali la Parte applica le misure di cui all'articolo 21. Ogni Pare dovrà considerare di ridurre questo tipo di riserva in modo da consentire l'applicazione più ampia possibile delle misure di cui all'articolo 20.

b. Qualora una Parte, a causa dei limiti previsti nella propria legislazione al momento dell'adozione della presente Convenzione, non è in grado di applicare le misure previste agli articoli 20 e 21 alle comunicazioni trasmesse in un sistema informatico di un *service provider* (fornitore di servizi), il cui sistema:

i. è operativo a vantaggio di un gruppo definito di utenti, e

ii. non utilizza reti di comunicazione pubblica e non è connesso con un altro sistema informatico, sia pubblico o che privato,

questa Parte si può riservare il diritto di non applicare queste misure a tali comunicazioni. Ogni Parte dovrà prevedere di ridurre tale riserva per consentire la più amplia applicazione possibile delle misure di cui agli articoli 20 e 21.

Articolo 15

Condizioni e tutele

1. Ogni Parte deve assicurarsi che l'instaurazione, implementazione e applicazione dei poteri e delle procedure previste in questa sezione siano soggette alle condizioni e alle tutele previste dal proprio diritto interno, che deve assicurare un'adeguata tutela dei diritti umani e delle libertà, in particolare dei diritti derivanti da obblighi assunti in base alla Convenzione del Consiglio d'Europa del 1950 per la tutela dei diritti umani e delle libertà fondamentali, alla Convenzione Internazionale delle Nazioni Unite del 1966 sui diritti civili e politici, e agli altri strumenti internazionali applicabili in materia di diritti umani, e che deve considerare il principio di proporzionalità.

2. Quando sia il caso, avuto riguardo alla natura del potere o della procedura, queste condizioni e tutele devono includere, fra l'altro, una supervisione giudiziaria o di altra natura purché indipendente, dei motivi che giustifichino l'applicazione e la limitazione del campo di applicazione e della durata del potere o procedura.

3. Nella misura in cui ciò sia rispondente all'interesse pubblico e, in particolare, alla buona amministrazione della giustizia, ogni Parte deve considerare l'impatto dei poteri e delle procedure di questa sezione sui diritti, le responsabilità e gli interessi legittimi dei terzi.

TITOLO II
CONSERVAZIONE RAPIDA DI DATI INFORMATICI IMMAGAZZINATI

Articolo 16
Conservazione rapida di dati informatici immagazzinati

1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per consentire alle competenti autorità di ordinare o ottenere in altro modo la protezione rapida di specifici dati informatici, inclusi i dati sul traffico, che sono stati conservati attraverso un sistema informatico, in particolare quando vi è motivo di ritenere che i dati informatici siano particolarmente vulnerabili e soggetti a cancellazione o modificazione.

2. Quando una Parte rende effettive le previsione di cui al precedente paragrafo 1. attraverso l'ordine ad un soggetto di conservare specifici dati informatici immagazzinati che siano in suo possesso o sotto il suo controllo, la Parte deve adottare le misure legislative e di altra natura che siano necessarie per obbligare tale soggetto a proteggere e mantenere l'integrità di quei dati informatici per il periodo di tempo necessario, per un massimo di novanta giorni, per consentire alle autorità competenti di ottenere la loro divulgazione. Una Parte può prevedere che tale ordine possa essere successivamente rinnovato.

3. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per obbligare il custode o la persona incaricata di conservare i dati informatici di mantenere il segreto sulla procedura intrapresa per il periodo di tempo previsto dal proprio diritto interno.

4. I poteri e le procedure di cui al presente articolo devono essere soggetti agli articoli 14 e 15.

Articolo 17
Conservazione e divulgazione rapide di dati relativi al traffico

1. Al fine di assicurare la conservazione dei dati relativi al traffico in applicazione di quanto previsto all'articolo 16 ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per:

a. assicurare che la conservazione dei dati relativi al traffico sia disponibile nonostante uno o più fornitori di servizi siano stati coinvolti nella trasmissione di tale comunicazione; e

b. assicurare la rapida trasmissione all'autorità competente della Parte, o al soggetto designato da tale autorità, di una quantità di dati relativi al traffico sufficiente per consentire alla Parte di identificare il fornitore di servizi e la via attraverso la quale la comunicazione fu trasmessa.

2. I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15.

TITOLO III
INGIUNZIONE DI PRODURRE

Articolo 18
Ingiunzione di produrre

1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per consentire alle autorità competenti di ordinare:

a. ad un soggetto nel proprio territorio di trasmettere specifici dati informatici nella propria disponibilità o controllo, che siano immagazzinati in un sistema informatico in un supporto informatico per la conservazione di dati; e

b. a un fornitore di servizi che offre le proprie presatazioni nel territorio della Parte di fornire i dati in proprio possesso o sotto il suo controllo relativi ai propri abbonati e concernenti tali servizi.

2. I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15.

3. Ai fini del presente articolo, l'espressione "informazioni relative agli abbonati" designa ogni informazione detenuta in forma di dato informatico o sotto altra forma da un fornitore di servizi e relativa agli abbonati ad un proprio servizio e diversa dai dati relativi al traffico o al contenuto e attraverso la quale è possibile stabilire:

a. il tipo di servizio di comunicazione utilizzato, le disposizioni tecniche prese a tale riguardo e il periodo del servizio;

b. l'identità dell'abbonato, l'indirizzo postale o geografico, il telefono e gli altri numeri d'accesso, i dati riguardanti la fatturazione e il pagamento, disponibili sulla base degli accordi o del contratto di fornitura del servizio;

c. ogni altra informazione sul luogo di installazione dell'apparecchiatura della comunicazione, disponibile sulla base degli accordi o del contratto di fornitura del servizio.

TITOLO IV
PERQUISIZIONE E SEQUESTRO DI DATI INFORMATICI IMMAGAZZINATI

Articolo 19
Perquisizione e sequestro dati informatici immagazzinati

1. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per consentire alle proprie autorità competenti di perquisire o accedere in modo simile:

a. a un sistema informatico o parte di esso e ai dati informatici ivi immagazzinati; e

b. a supporto per la conservazione di dati informatici nel quale i dati stessi possono essere immagazzinati nel proprio territorio.

2. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire che, qualora le proprie autorità perquisiscano o accedano in modo simile a specifici sistemi informatici o parte di essi, in conformità al paragrafo 1.a, e abbiano ragione di ritenere che i dati ricercati si trovino presso un altro sistema informatico o parte di esso nel proprio territorio, e a tali dati sia possibile legalmente l'accesso dal sistema iniziale, le stesse autorità possano estendere rapidamente la perquisizione o l'accesso all'altro sistema.

3. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie autorità competenti di sequestrare o acquisire in modo simile i dati informatici per i quali si è proceduto all'accesso in conformità ai paragrafi 1 o 2. Tali misure devono includere il potere di:

a. sequestrare o acquisire in modo simile un sistema informatico o parte di esso o un supporto per la conservazione di dati informatici;

b. fare e trattenere una copia di quei dati informatici ;

c. mantenere l'integrità dei relativi dati informatici immagazzinati;

d. rendere inaccessibile o rimuovere quei dati dal sistema informatico analizzato.

4. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie competenti autorità di ordinare ad ogni soggetto che abbia conoscenza del funzionamento del sistema informatico o delle misure utilizzate per proteggere i dati informatici in esso contenuti, di mettere a disposizione tutte le informazioni ragionevolmente necessarie per consentire l'applicazione delle misure di cui ai paragrafi 1. e 2.

5. I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15.

TITOLO V
RACCOLTA IN TEMPO REALE DI DATI INFORMATICI

Articolo 20
Raccolta in tempo reale di dati sul traffico

1. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per consentire alle proprie competenti autorità di:

a. raccogliere o registrare attraverso l'utilizzo di strumenti tecnici nel suo territorio;

b. obbligare un fornitore di servizi, nell'ambito delle sue capacità tecniche a:

i. raccogliere o registrare attraverso l'utilizzo di strumenti tecnici esistenti nel suo territorio, o

ii. cooperare ed assistere le autorità competenti nella raccolta o registrazione in tempo reale di dati sul traffico associati a comunicazioni specifiche effettuate sul proprio territorio attraverso un sistema informatico.

2. Qualora una Parte, a causa dei limiti previsti dal proprio ordinamento giuridico, non è in grado di applicare le misure previste al paragrafo 1.a, può, invece, adottare le misure legislative o di altra natura che dovessero essere necessarie per consentire la raccolta o la registrazione in tempo reale dei dati relativi al traffico associati a comunicazioni specifiche effettuate sul proprio territorio, attraverso l'utilizzo di strumenti tecnici esistenti su questo territorio.

3. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per obbligare un fornitore di servizi a mantenere segreti il fatto che un qualsiasi potere previsto nel presente articolo sia stato esercitato e ogni informazione relativa.

I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15.

Articolo 21
Intercettazione di dati relativi al contenuto

1. Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie, in relazione ad una serie di gravi infrazioni che devono essere definite dal diritto nazionale, per consentire alle proprie competenti autorità di:

a. raccogliere o registrare attraverso l'utilizzo di strumenti tecnici esistenti nel territorio della Parte, e

b. obbligare un fornitori di servizi, nell'ambito delle sue capacità tecniche a:

i. raccogliere o registrare attraverso l'utilizzo di strumenti tecnici esistenti nel territorio della Parte, o

II. cooperare ed assistere le autorità competenti nella raccolta o registrazione in tempo reale di dati relativi al contenuto di comunicazioni specifiche eseguite nel proprio territorio attraverso un sistema informatico.

2. Qualora una Parte, a causa dei principi del proprio ordinamento giuridico, non è in grado di applicare le misure previste al paragrafo 1.a, può invece adottare misure legislative e di altra natura che dovessero essere necessarie per assicurare la raccolta o la registrazione in tempo reale dei dati relativi al contenuto di comunicazioni specifiche eseguite sul proprio territorio, attraverso l'utilizzo di strumenti tecnici in quel territorio.

3. Ogni Parte deve adottare le misure legislative ed di altra natura che dovessero essere necessarie per obbligare un fornitore di servizi a mantenere segreto il fatto che un qualsiasi potere previsto nel presente articolo sia stato sia stato esercitato e ogni informazione relativa.

4.I poteri e le procedure di cui al presente articolo devono essere soggette agli articoli 14 e 15.

SEZIONE III
COMPETENZA

Articolo 22
Competenza

1.Ogni Parte deve adottare le misure legislative e di altra natura che dovessero essere necessarie per stabilire la propria competenza per tutti i reati previsti in conformità agli articoli da 2 a 11 della presente Convenzione, quando i reati siano commessi:

a. nel proprio territorio;

b. a bordo di una nave battente bandiera della Parte;

c. a bordo di un aeromobile immatricolato presso quella Parte;

d. da un proprio cittadino, se l'infrazione è penalmente punibile la dove è stata commessa o se l'infrazione non rientra nella competenza territoriale di alcuno Stato.

2. Ogni Parte può riservarsi il diritto di non applicare o di applicare solo in condizioni o casi specifici le regole di competenza definite ai paragrafi 1.b - 1.d del presente articolo o in una parte qualunque di essi.

3. Ogni Parte deve adottare le misure che dovessero essere necessarie per stabilire la propria competenza in ordine alle infrazioni di cui all'articolo 24, paragrafo 1 della presente Convenzione, nel caso in cui l'autore presunto dell'infrazione si trovi nel proprio territorio e

non è estradabile verso un'altra Parte solo in virtù della sua nazionalità, dopo una richiesta di estradizione.

4. La presente Convenzione non esclude alcuna competenza penale esercitata da una Parte in base al proprio diritto interno.

5. Quando più di una Parte rivendica la propria competenza per una presunta infrazione prevista dalla presente Convenzione, le Parti coinvolte si consultano, laddove sia opportuno, al fine di stabilire la competenza più appropriata per esercitare l'azione penale.

CAPITOLO III
COOPERAZIONE INTERNAZIONALE

SEZIONE II
PRINCIPI GENERALI

TITOLO I
PRINCIPI GENERALI RELATIVI ALLA COOPERAZIONE INTERNAZIONALE

Articolo 23
Principi generali relativi alla cooperazione internazionale

Le parti devono cooperare tra loro nella misura più ampia possibile nelle indagini o nei procedimenti riguardanti i reati collegati a sistemi e dati informatici, o per raccogliere le prove, in forma elettronica, di un reato, in conformità alle disposizioni di questo capitolo e in applicazione degli strumenti internazionali sulla cooperazione internazionale in materia penale, degli accordi stipulati sulla base di una legislazione uniforme o in condizione di reciprocità e del loro diritto nazionale.

TITOLO II
PRINCIPI RELATIVI ALL'ESTRADIZIONE

Articolo 24
Estradizione

1. a. Il presente articolo si applica all'estradizione tra Parti per i reati stabiliti in base agli articoli da 2 a 11 della presente Convenzione, a condizione che essi siano punibili in base

alla legge di entrambe le Parti con la privazione della libertà per un periodo massimo di almeno un anno, o con una pena più severa.

b. Qualora sia richiesta una pena minima differente in base ad un trattato di estradizione applicabile fra due o più parti, ivi compresa la Convenzione Europea d'Estradizione (STE No. 24) o in forza di un accordo stipulato sulla base di legislazioni uniformi o reciproche, si applica la pena minima prevista in base a questi trattati o accordi.

2. I reati descritti al paragrafo 1 del presente articolo devono essere considerati come inclusi nel novero dei reati che possono dar luogo ad estradizione in tutti i trattati di estradizione esistenti tra le Parti. Le Parti si impegnano ad includere tali reati fra quelli che possono comportare l'estradizione in ogni trattato di estradizione che sarà concluso tra di esse.

3. Qualora una Parte condizioni l'estradizione all'esistenza di un trattato e riceva una richiesta di estradizione di un'altra Parte con la quale non ha un trattato di estradizione, la presente Convenzione può essere considerata come base giuridica per l'estradizione nei riguardi di tutti i reati menzionati al paragrafo 1 del presente articolo.

4. Le Parti che non condizionano l'estradizione all'esistenza di un trattato devono considerare i reati menzionati al paragrafo 1 del presente articolo come reati che possono dar luogo ad estradizione tra di esse.

5. L'estradizione è soggetta alle condizioni previste dal diritto interno della Parte richiedente o dai trattati di estradizione in vigore, inclusi i motivi in base ai quali la Parte richiesta può rifiutare di concedere l'estradizione.

6. Qualora l'estradizione per un reato menzionata al paragrafo 1 del presente articolo venga rifiutata esclusivamente sulla base della nazionalità della persona ricercata, o perché la Parte richiesta eccepisce la propria competenza per quel reato, la Parte richiesta deve sottoporre il caso su richiesta della Parte richiedente alla proprie autorità competenti a procedere e dovrà trasmettere i risultati finali alla Parte richiedente in tempo utile. Tali autorità dovranno prendere le proprie decisioni e condurre le proprie indagini e i procedimenti allo stesso che per tutti gli altri reati comparabili per natura in base alla legislazione di tale Parte.

7. a. Ogni Parte, al momento della firma o del deposito dello strumento di ratifica, di accettazione, di approvazione o di adesione, deve comunicare al Segretariato Generale del Consiglio d'Europa il nome e l'indirizzo di ogni autorità responsabile dell'invio o della ricezione delle richieste di estradizione o di arresto provvisorio in mancanza di un trattato.

b. Il Segretariato Generale del Consiglio d'Europa deve istituire e aggiornare un registro delle autorità a tal fine designate dalle Parti. Ogni Parte deve assicurare che i dati del registro siano corretti in ogni momento.

TITOLO III
PRINCIPI GENERALI RELATIVI ALLA MUTUA ASSISTENZA

Articolo 25
Principi generali relativi alla mutua assistenza

1. Le Parti devono concedersi reciprocamente la più ampia mutua assistenza al fine delle indagini o dei procedimenti relativi ai reati relativi a sistemi e dati informatici o per la raccolta di prove in formato elettronico di reati.

2. Ogni Parte deve anche adottare le misure legislative ed di altra natura che dovessero essere necessarie per l'adempimento degli obblighi assunti in base agli articoli da 27 al 35.

3. Ogni Parte può, in casi d'urgenza, fare richieste di mutua assistenza o comunicazioni ad essa relative attraverso strumenti rapidi di comunicazione, come il fax o la posta elettronica, a condizione che tali strumenti diano appropriate garanzie di sicurezza e autenticazione (inclusa la criptazione, se necessaria), seguite da conferma ufficiale ulteriore se lo Stato richiesto lo esige. Lo Stato richiesto deve accettare la domanda e rispondere alla richiesta con uno qualsiasi di tali mezzi rapidi di comunicazione.

4. Salva contraria disposizione espressamente prevista negli articoli del presente capitolo, la mutua assistenza è soggetta alle condizioni previste dalla legislazione della Parte richiesta o dai trattati di mutua assistenza applicabili, inclusi i motivi sulla base dei quali la Parte richiesta può rifiutare la cooperazione. La Parte richiesta non può esercitare il diritto di rifiutare la mutua assistenza in relazione ai reati menzionati negli articoli da 2 a 11 per il solo motivo che la richiesta riguarda un reato che essa reputa di natura fiscale.

5. Qualora, in conformità alle previsioni del presente capitolo, la Parte richiesta è autorizzata a subordinare la mutua assistenza ad una doppia incriminazione, questa condizione sarà considerata come soddisfatta, se il comportamento considerato reato per il quale la mutua assistenza è stata richiesta costituisca reato in base al proprio diritto interno, a prescindere dal fatto che la propria legislazione classifichi o meno il reato nella stessa categoria o lo denomini con la stessa terminologia della legislazione della Parte richiedente.

Articolo 26
Informazioni spontanee

1. Una Parte può, nei limiti della propria legislazione nazionale e senza una richiesta preventiva, trasmettere ad un'altra Parte informazioni ottenute nell'ambito delle proprie indagini qualora ritenga che la comunicazione di tali informazioni possa aiutare la Parte ricevente nell'avvio o nello svolgimento di indagini o procedimenti riguardanti reati definiti in

base alla presente Convenzione o possa giovare ad una richiesta di quella Parte in base al presente capitolo.

2. Prima di trasmettere tali informazioni, la Parte trasmittente può richiedere che esse vengano mantenute confidenziali o usate solo a determinate condizioni. Qualora la Parte ricevente non possa adeguarsi a tale richiesta, essa deve informare l'altra Parte, che dovrà quindi stabilire se le informazioni debbano comunque essere trasmesse. Qualora la Parte ricevente accetti le informazioni alle condizioni stabilite, essa dovrà attenervisi.

TITOLO IV
PROCEDURE RELATIVE ALLE RICHIESTE DI MUTUA ASSISTENZA IN ASSENZA DI ACCORDI INTERNAZIONALI APPLICABILI

Articolo 27
Procedure relative alle richieste di mutua assistenza in assenza di accordi internazionali applicabili

1. Qualora non vi sia un trattato o un accordo di mutua assistenza concluso sulla base di una legislazione uniforme in vigore o in condizione di reciprocità tra la Parte richiedente e richiesta, si applicano le disposizioni dei paragrafi da 2 a 9 del presente articolo. Le stesse non si applicano qualora vi sia un trattato, accordo o legislazione in vigore, a meno che le Parti interessate siano d'accordo nell'applicare a loro posto in tutto o in parte questo articolo.

2. a. Ogni Parte deve designare un'autorità centrale responsabile dell'invio e delle risposte alle richieste di mutua assistenza, dell'esecuzione di tali richieste o della loro trasmissione alle autorità competenti per la loro esecuzione.

b. Le autorità centrali devono comunicare direttamente tra loro;

c. Ogni Parte, al momento della firma o del deposito dello strumento di ratifica, di accettazione, di approvazione o di adesione, deve comunicare al Segretariato Generale del Consiglio d'Europa il nome e l'indirizzo dell'autorità designata in applicazione del presente paragrafo;

d. Il Segretariato Generale del Consiglio d'Europa deve istituire e tenere aggiornato un registro delle autorità centrali designate dalle Parti. Ogni Parte deve assicurare che i dati del registro siano corretti in ogni momento.

3. Le domande di mutua assistenza avanzate in base al presente articolo devono essere eseguite in conformità alle procedure specificate dalla Parte richiedente, salvo che siano incompatibili con la legislazione della Parte richiesta.

4. La Parte richiesta può, in aggiunta ai motivi di rifiuto stabiliti dall'articolo 25, paragrafo 4, rifiutare l'assistenza se:

a. la richiesta riguarda un reato che la Parte richiesta considera politico o connesso con un reato politico, o

b. la Parte richiesta ritenga che l'esecuzione della richiesta possa recare pregiudizio alla propria sovranità, alla sua sicurezza, all'ordine pubblico o ad altri interessi essenziali.

5. La Parte richiesta può sospendere l'esecuzione di una richiesta se la stessa può pregiudicare indagini o procedimenti condotti dalle proprie autorità.

6. Prima di rifiutare o sospendere l'assistenza, la Parte richiesta deve, se del caso dopo essersi consultata con la Parte richiedente, considerare se la richiesta possa essere eseguita in parte o sottoposta alle condizioni che ritenga necessarie.

7. La Parte richiesta deve prontamente informare la Parte richiedente del seguito che intende dare alla richiesta di assistenza. Essa dovrà motivare ogni rifiuto o sospensione della richiesta. La Parte richiesta deve anche informare la Parte richiedente di tutte le motivazioni che rendono impossibile l'esecuzione della richiesta o che sono in grado di ritardarla in modo significativo.

8. La Parte richiedente può richiedere che la Parte richiesta mantenga confidenziale il fatto e anche l'oggetto di ogni richiesta fatta in base al presente capitolo, salvo nella misura in cui sia necessario per la sua esecuzione. Qualora la Parte richiesta non possa adeguarsi la richiesta di confidenzialità, essa deve prontamente informare l'altra Parte, che dovrà quindi stabilire se la richiesta debba comunque essere eseguita.

9. a. In caso di urgenza, le richieste di mutua assistenza o le comunicazione ad essa collegate possono essere trasmesse direttamente alle autorità giudiziarie della Parte richiedente dalle autorità della Parte richiesta. In tale caso, una copia deve essere trasmessa contemporaneamente all'autorità centrale della Parte richiesta attraverso l'autorità centrale della Parte richiedente.

b. Ogni richiesta o comunicazione in base al presente paragrafo può essere effettuata attraverso l'Organizzazione Internazionale della Polizia Criminale (Interpol).

c. Qualora una richiesta venga effettuata in base al punto a. del presente articolo e l'autorità non sia competente ad esaminarla, essa deve trasmetterla all'autorità nazionale competente ed informarne direttamente la Parte richiedente.

d. Le richieste o le comunicazioni effettuate in base a questo paragrafo che non implichino azioni coercitive possono essere direttamente trasmesse dalle autorità competenti della Parte richiedente alle autorità competenti della Parte richiesta.

e. Ogni Parte può, al momento della firma o del deposito dello strumento di ratifica, di accettazione, di approvazione o di adesione, comunicare al Segretariato Generale del

Consiglio d'Europa che, per ragioni di efficienza, le richieste effettuate in base al presente paragrafo dovranno essere indirizziate alla propria autorità centrale.

Articolo 28

Confidenzialità e limitazioni di utilizzo

1. Quando non vi è un trattato o un accordo di mutua assistenza sulla base di una legislazione uniforme o in condizione di reciprocità in vigore tra la Parte richiedente e la Parte richiesta, devono applicarsi le disposizioni del presente articolo. Le disposizioni del presente articolo non si applicano qualora vi sia un trattato, accordo o legislazione in vigore, a meno che le Parti interessate siano d'accordo nell'applicare a loro posto in tutto o in parte il presente articolo.

2. La Parte richiesta può subordinare la comunicazione di informazioni o materiali in risposta ad una richiesta alla condizione che :

a. vengano mantenute confidenziali qualora la richiesta di mutua assistenza legale non possa essere soddisfatta in mancanza di tale condizione; o

b. non vengano utilizzate per indagini o procedimenti diversi da quelli indicati nella richiesta.

3. Qualora la Parte richiedente non possa soddisfare una delle condizioni contenute nel paragrafo 2, essa deve prontamente informare l'altra Parte, che deve stabilire se l'informazione possa comunque essere trasmessa. Quando la Parte richiedente accetta la condizione, essa vi si dovrà attenere.

4. Ogni Parte che fornisca un'informazione o del materiale soggetto ad una condizione in base al paragrafo 2 può richiedere all'altra Parte precisazioni, in relazione a tale condizione, circa l'uso fatto di tale informazione o materiale.

SEZIONE II

DISPOSIZIONI SPECIFICHE

TITOLO I

MUTUA ASSISTENZA RELATIVA A MISURE PROVVISORIE

Articolo 29

Conservazione rapida di dati informatici immagazzinati

1. Una Parte può richiedere ad un'altra Parte di ordinare od ottenere in altro modo la conservazione rapida di dati immagazzinati attraverso un sistema informatico, situato nel

territorio di quest'altra Parte e nei confronti della quale la Parte richiedente intende avanzare una richiesta di mutua assistenza per la perquisizione o altro simile mezzo di accesso, per il sequestro o altro strumento simile, o per la divulgazione dei dati.

2. Una richiesta di conservazione effettuata in base al paragrafo 1 deve specificare:

a. l'autorità che richiede la conservazione;

b. il reato che costituisce oggetto di indagine e una breve esposizione dei fatti relativi;

c. i dati informatici immagazzinati da conservare e il loro legame con il reato;

d. tutte le informazioni utili ad identificare il custode dei dati informatici immagazzinati o il luogo dove si trova il sistema informatico;

e. la necessità della conservazione; e

f. che la Parte intende avanzare una richiesta di mutua assistenza per la perquisizione o altro simile mezzo di accesso, per il sequestro o uno strumento similare, o per la divulgazione dei dati.

3. Dopo aver ricevuto la richiesta da un'altra Parte, la Parte richiesta deve prendere tutte le misure appropriate per conservare rapidamente i dati specificati in base alla propria legge nazionale. Per rispondere ad una tale richiesta, la doppia incriminazione non è richiesta come condizione per provvedere alla conservazione.

4. Una Parte che richiede la doppia incriminazione come condizione di procedibilità per rispondere ad una richiesta di mutua assistenza per la perquisizione o altro simile mezzo di accesso, per il sequestro o altro strumento similare, o per la divulgazione dei dati immagazzinati può, riguardo a reati diversi da quelli definiti in base agli articoli da 2 a 11 della presente Convenzione, riservarsi il diritto di rifiutare la richiesta di conservazione in base al presente articolo, nei casi in cui ha ragione di ritenere che, al momento della divulgazione, la condizione della doppia incriminazione non possa realizzarsi.

5. Inoltre, una richiesta di conservazione può essere rifiutata solo se:

a. la richiesta è relativa ad un reato che la Parte richiesta considera un reato politico o un reato connesso ad un reato politico; o

b. la Parte richiesta ritenga che l'esecuzione della richiesta possa recare pregiudizio alla propria sovranità, alla sua sicurezza, all'ordine pubblico o ad altri interessi essenziali.

6. Qualora la Parte richiesta ritenga che la conservazione non assicurerà la disponibilità in futuro dei dati o comprometterà la confidenzialità o pregiudicherà in altro modo le indagini della Parte richiedente, essa deve prontamente informare la Parte richiedente che dovrà decidere se la richiesta vada comunque eseguita.

7. Tutte le conservazioni effettuate a seguito di una richiesta di cui al paragrafo 1 devono essere disponibili per un periodo non inferiore a sessanta giorni, al fine di permettere alla Parte richiedente di effettuare una richiesta per la perquisizione o altro simile mezzo di accesso, per il sequestro o altro strumento analogo, o per la divulgazione dei dati. A seguito

del ricevimento di tale richiesta, i dati dovranno continuare ad essere conservati in attesa della decisione su tale richiesta

Articolo 30

Divulgazione rapida di dati di traffico conservati

1. Qualora, nel corso dell'esecuzione di una richiesta effettuata sulla base dell'articolo 29 per conservare dati sul traffico relativi ad una specifica comunicazione, la Parte richiesta scopra che un *service provider* di un altro Stato sia coinvolto nella trasmissione della comunicazione, la Parte richiesta deve rapidamente trasmettere alla Parte richiedente una quantità sufficiente di dati concernenti il traffico che consenta di identificare il *service provider* e la via attraverso la quale la comunicazione fu effettuata.

2. La divulgazione di dati di traffico di cui al paragrafo 1 può essere rifiutata solo se:

a. la richiesta riguarda un reato che la Parte richiesta consideri un reato politico o un reato connesso ad un reato politico; o

b. la Parte richiesta ritenga che l'esecuzione della richiesta possa recare pregiudizio alla propria sovranità, alla sua sicurezza, al proprio ordine pubblico o ad altri interessi essenziali.

TITOLO II

MUTUA ASSISTENZA RELATIVA AI POTERI D'INDAGINE

Articolo 31

Mutua assistenza concernente l'accesso a dati informatici immagazzinati

1. Una Parte può richiedere ad un'altra Parte la perquisizione o altro simile mezzo di accesso, il sequestro o altro strumento simile, o la divulgazione dei dati immagazzinati attraverso un sistema informatico situato nel territorio della Parte richiesta, inclusi i dati che sono stati conservati in base all'articolo 29.

2. La Parte richiesta soddisfa la richiesta attraverso gli strumenti internazionali, gli accordi e le legislazioni alle quali si fa riferimento all'articolo 23, e conformandosi alle disposizioni del presente capitolo.

3. La richiesta deve essere soddisfatta al più presto possibile quando:

a. vi è motivo di ritenere che i dati relativi siano particolarmente a rischio di perdita o modificazioni; o

b. gli strumenti, gli accordi e le legislazione di cui al paragrafo 2 prevedano una cooperazione rapida.

Articolo 32

Accesso transfrontaliero a dati informatici immagazzinati con il consenso o quando pubblicamente disponibili

Una Parte può, senza l'autorizzazione di un'altra Parte:

a. accedere ai dati informatici immagazzinati disponibili al pubblico (fonti aperte), senza avere riguardo al luogo geografico in cui si trovano tali dati; o

b. accedere o ricevere, attraverso un sistema informatico nel proprio territorio, dati informatici immagazzinati situati in un altro Stato, se la Parte ottiene il consenso legale e volontario della persona legalmente autorizzata a divulgare i dati allo Stato attraverso tale sistema informatico.

Articolo 33

Mutua assistenza nella raccolta in tempo reale di dati sul traffico

1. Le Parti devono fornire mutua assistenza tra loro nella raccolta in tempo reale di dati sul traffico, associati a specifiche comunicazioni nel proprio territorio, trasmessi attraverso l'uso di un sistema informatico. Questa assistenza, soggetta alle disposizioni del paragrafo 2, è regolata dalle condizioni e dalle procedure previste dal diritto interno.

2. Tutte le Parti devono fornire questa assistenza almeno rispetto ai reati per i quali la raccolta in tempo reale dei dati sul traffico sarebbe possibile, in ambito interno, in una situazione analoga.

Articolo 34

Mutua assistenza in materia di intercettazione di dati relativi al contenuto

Le Parti devono fornirsi mutua assistenza nella raccolta o registrazione in tempo reale di dati relativi al contenuto di specificate comunicazioni trasmesse attraverso l'uso di un sistema informatico nella misura consentita dai trattati applicabili fra le stesse e dalle leggi interne.

TITOLO III

RETE 24/7

Articolo 35

Rete 24/7

1. Ogni Parte deve designare un punto di contatto disponibile 24 ore su 24 e 7 giorni su 7, per assicurare un'assistenza immediata per le indagini relative a reati connessi a sistemi e

dati informatici, o per la raccolta di prove in formato elettronico di un reato. Tale assistenza deve includere la facilitazione o, se il diritto interno e la prassi nazionale lo consentono, l'applicazione diretta delle seguenti misure:

a. apporto di consigli tecnici;

b. conservazione dei dati in base agli articoli 29 e 30;

c. raccolta di prove, trasmissione di informazioni di carattere giuridico e localizzazione dei sospetti.

2. a. Il punto di contatto di una Parte deve poter comunicare con il punto di contatto di un'altra Parte secondo una procedura accelerata.

b. Se il punto di contatto designato da una Parte non dipende dall'autorità della Parte o delle autorità responsabili per la mutua assistenza internazionale o per l'estradizione, il punto di contatto dovrà garantire di essere in grado di coordinarsi con quella o con queste secondo una procedura accelerata.

3. Ogni Parte farà in modo di disporre di personale formato ed equipaggiato al fine di facilitare le attività della rete.

CAPITOLO IV
DISPOSIZIONI FINALI

Articolo 36
Firma ed entrata in vigore

1. Questa Convenzione è aperta alla firma degli Stati membri del Consiglio d'Europa e degli Stati non membri che hanno partecipato alla sua elaborazione.

2. Questa Convenzione è soggetta a ratifica, accettazione o approvazione. Gli strumenti di ratifica, accettazione o approvazione devono essere depositati presso il Segretariato Generale del Consiglio d'Europa.

3. Questa Convenzione entrerà in vigore il primo giorno del mese successivo alla scadenza dei tre mesi successivi alla data in cui cinque Stati, compresi almeno tre Stati membri del Consiglio d'Europa, avranno espresso il loro consenso ad essere vincolati dalla Convenzione conformemente alle disposizioni dei paragrafi 1 e 2.

4. Nei confronti di ogni Stato firmatario che esprima successivamente il proprio consenso, la Convenzione entrerà in vigore il primo giorno successivo la scadenza dei tre mesi successivi la data in cui viene espresso il consenso in conformità alle disposizioni dei paragrafi 1 e 2.

Articolo 37
Adesione alla Convenzione

1. Dopo l'entrata in vigore della presente Convenzione, il Comitato dei Ministri del Consiglio d'Europa, dopo avere consultato gli Stati Contraenti e dopo averne ottenuto il consenso unanime, può invitare ogni Stato che non sia membro del Consiglio e che non abbia partecipato alla elaborazione della Convenzione ad aderirvi. La decisione può essere presa a maggioranza secondo la disposizione dell'articolo 20.d. dello Statuto del Consiglio d'Europa e con voto unanime dei rappresentanti degli Stati contraenti aventi titolo a sedere nel Comitato dei Ministri.

2. Nei confronti di tutti gli Stati che abbiano aderito alla Convenzione in base al paragrafo 1. di cui sopra, la Convenzione entrerà in vigore il primo giorno del mese successivo alla scadenza dei tre mesi successivi alla data di deposito dello strumento di adesione presso il Segretariato Generale del Consiglio d'Europa.

Articolo 38
Applicazione territoriale

1. Ogni Stato può, al momento della firma o quando depositi il proprio strumento di ratifica, accettazione, approvazione o adesione, specificare il territorio o i territori ai quali la Convenzione si applica.
2. Ogni Stato può, successivamente, attraverso una dichiarazione indirizzata al Segretariato Generale del Consiglio d'Europa, estendere l'applicazione della Convenzione ad ogni altro territorio specificato nella dichiarazione. Nell'ambito di tale territorio la Convenzione entrerà in vigore il primo giorno del mese successivo alla scadenza di un periodo di tre mesi dalla data di ricevimento della dichiarazione da parte del Segretariato Generale.
3. Ogni dichiarazione effettuata in base ai due precedenti paragrafi può, nell'ambito di ogni territorio specificato in tale dichiarazione, essere revocata attraverso una notifica indirizzata al Segretariato Generale del Consiglio d'Europa. La revoca avrà effetto dal primo giorno del mese successivo alla scadenza di un periodo di tre mesi dalla data di ricevimento di tale notifica da parte del Segretariato Generale.

Articolo 39
Effetti della Convenzione

1. Lo scopo della presente Convenzione è quello di completare i trattati e gli accordi multilaterali e bilaterali applicabili esistenti tra le Parti, incluse le disposizioni:

- della Convenzione europea sull'estradizione, aperta alla firma a Parigi, il 13 dicembre 1957 (ETS n. 24);

- della Convenzione europea sulla mutua assistenza in campo penale, aperta alla firma a Strasburgo, il 20 aprile 1959 (ETS n. 30);
- del Protocollo addizionale della Convenzione europea sulla mutua assistenza in campo penale, aperto alla firma a Strasburgo, il 17 MARZO 1978 (ETS n. 99).

2. Qualora due o più Parti abbiano già concluso un accordo o un trattato sulla materia trattata dalla presente Convenzione o abbiano in altro modo regolato le proprie relazioni su tali materie, o dovessero farlo in futuro, esse avranno anche facoltà d'applicare tale accordo o trattato o regolare le loro relazioni di conseguenza, in luogo della presenta Convenzione. Tuttavia, qualora le Parti stabiliscano le loro relazioni relative alle materie trattate nella presente Convenzione in modo diverso, esse dovranno farlo in modo che non sia incompatibile con l'oggetto e i principi della Convenzione.

3. Niente della presente Convenzione riguarda altri diritti, restrizioni, obbligazioni e responsabilità di una Parte.

Articolo 40

Dichiarazioni

Attraverso una dichiarazione scritta indirizzata al Segretariato Generale del Consiglio d'Europa, ogni Stato può, al momento della firma o quando depositi il proprio strumento di ratifica, accettazione, approvazione o adesione, dichiarare che si riserva la facoltà di richiedere elementi ulteriori come disposto dagli articoli 2, 3, 6 paragrafo 1 (b), 7, 9, paragrafo 3 e 27, paragrafo 9 (e).

Articolo 41

Clausola federale

1. Uno Stato federale può riservarsi il diritto di onorare gli impegni assunti in base al capitolo II della presente Convenzione nella misura in cui siano compatibili con i principi fondamentali che regolano i rapporti tra il proprio governo centrale e gli Stati membri o altre entità territoriali simili, a condizione che esso sia in grado di cooperare in base al capitolo III.

2. Quando effettua una riserva in base al paragrafo 1., uno Stato federale non può applicare i termini di tale riserva per escludere o diminuire sostanzialmente i propri obblighi di cui al capitolo II. In ogni caso, esso deve dotarsi di mezzi estesi ed effettivi che permettano la messa in opera delle misure previste da detto capitolo.

3. Nei riguardi delle disposizioni di questa Convenzione la cui applicazione ricade sotto la competenza di ciascuno Stato membro o di altra entità territoriale simile, che in base al sistema costituzionale della federazione non sia obbligato a prendere misure legislative, il governo federale deve informare le autorità competenti di tali Stati delle suddette

disposizioni, esprimendo parere favorevole e incoraggiandolo ad assumere iniziative adeguate per darvi esecuzione.

Articolo 42

Riserve

Con una notifica scritta indirizzata al Segretariato Generale del Consiglio d'Europa, ogni Stato può, al momento della firma o quando depositi il proprio strumento di ratifica, accettazione, approvazione o adesione, dichiarare che si avvale della riserva o delle riserve di cui all'articolo 4, paragrafo 2, articolo 6, paragrafo 3, articolo 9, paragrafo 4, articolo 10, paragrafo 3, articolo 11, paragrafo 3, articolo 14, paragrafo 3, articolo 22, paragrafo 2, articolo 29, paragrafo 4 e articolo 41, paragrafo 1. Non sono ammissibili altre riserve.

Articolo 43

Status e cancellazione delle riserve

1. La Parte che abbia formulato una riserva in conformità all'articolo 42 può ritirarla in tutto in parte inviando una notifica al Segretariato Generale del Consiglio d'Europa. Tale ritiro avrà effetto dalla data di ricevimento di tale notifica da parte del Segretariato Generale. Qualora la notifica indichi che il ritiro avrà effetto da una data specifica in essa indicata e tale data è successiva alla data della notifica, il ritiro ha effetto in tale data.
2. La Parte che abbia fatto una riserva come stabilito all'articolo 42 può ritirarla, in tutto o in parte, non appena le circostanze lo permettano.
3. Il Segretariato Generale del Consiglio d'Europa può periodicamente domandare alle Parti che hanno fatto una o più riserve di cui all'articolo 42 le prospettive del ritiro di tali riserve.

Articolo 44

Emendamenti

1. Emendamenti alla presente Convenzione possono essere proposti da ogni Parte e devono essere comunicati dal Segretariato Generale del Consiglio d'Europa agli Stati membri del Consiglio d'Europa, agli Stati non membri che hanno partecipato alla sua elaborazione e ad ogni Stato che vi ha aderito o è stato invitato ad aderirvi in conformità alle disposizioni dell'articolo 37.
2. Ogni emendamento proposto da una Parte deve essere comunicato al Comitato Europeo per i Problemi Criminali (CDPC), che dovrà sottoporre al Comitato dei Ministri il proprio parere su tale proposta di emendamento.
3. Il Comitato dei Ministri deve esaminare l'emendamento proposto e l'avviso espresso dal Comitato Europeo per i Problemi Criminali (CDPC) e, a seguito di consultazione degli Stati non membri Parti della presente Convenzione, può adottare l'emendamento.

4. Il testo di ogni emendamento adottato dal Comitato dei Ministri in conformità al paragrafo 3. del presente articolo deve essere trasmesso alle Parti per accettazione.

5. Ogni emendamento adottato in conformità al paragrafo 3. del presente articolo entrerà in vigore il trentesimo giorno dopo che tutte le Parti hanno informato il Segretariato Generale della loro accettazione.

Articolo 45

Risoluzione dei contrasti

Il Comitato Europeo per i Problemi Criminali (CDPC) deve essere informato della interpretazione e dell'applicazione della presente Convenzione.

Nel caso di un contrasto tra le Parti sull'interpretazione o applicazione della presente Convenzione, le Parti stesse si adopereranno per trovare una soluzione attraverso negoziati o con ogni altro pacifico strumento a loro scelta, inclusa la sottoposizione del contrasto al Comitato Europeo per i Problemi Criminali, ad un tribunale arbitrale la cui decisione sarà vincolante per le Parti, o alla Corte Internazionale di Giustizia, come concordato dalle Parti coinvolte.

Articolo 46

Consultazione delle Parti

1. Le Parti devono, quando occorra, consultarsi periodicamente allo scopo di facilitare:

a. l'effettivo uso e l'esecuzione della presente Convenzione, inclusa l'individuazione di ogni problema in materia, così come gli effetti di ogni dichiarazione o riserva fatta riguardo alla presente Convenzione;

b. lo scambio di informazioni sugli sviluppi legislativi, politici o tecnologici riguardanti la criminalità informatica e la raccolta di prove in formato elettronico;

c. l'esame di eventuali integrazioni o emendamenti della Convenzione.

2. Il Comitato Europeo per i Problemi Criminali (CDPC) deve essere mantenuto periodicamente informato dei risultati delle consultazioni di cui al paragrafo 1.

3. Il Comitato Europeo per i Problemi Criminali (CDPC) deve, quando occorra, facilitare le consultazioni di cui al paragrafo 1. e prendere le misure necessarie per assistere le Parti nel loro sforzo di integrare o modificare la Convenzione. Non oltre un triennio dall'entrata in vigore della Convenzione, il Comitato Europeo per i Problemi Criminali (CDPC) deve, in cooperazione con le Parti, procedere ad un riesame di tutte le disposizioni della Convenzione e, se necessario, consigliare tutte le modifiche opportune.

4. Salvi i casi in cui vengano assunte dal Consiglio d'Europa, le spese affrontate per l'esecuzione delle disposizioni del paragrafo 1. devono essere sostenute dalle Parti nel modo da esse stabilito.

5. Le Parti devono essere assistite dal Segretariato del Consiglio d'Europa nell'esercizio delle loro funzioni in base al presente articolo.

Articolo 47

Denuncia

1. Tutte le Parti possono, in ogni momento, denunciare la presente Convenzione attraverso la notifica al Segretariato Generale del Consiglio d'Europa.

2. Tale denuncia produce effetto a partire dal primo giorno del mese successivo alla scadenza di un periodo di tre mesi dalla data di ricevimento della notifica da parte del Segretariato Generale.

Articolo 48

Notificazione

Il Segretariato Generale del Consiglio d'Europa dovrà notificare ad ogni Stato membro del Consiglio d'Europa, agli Stati non membri che hanno partecipato nell'elaborazione della presente Convenzione e ad ogni Stato che vi ha aderito o è stato invitato ad aderirvi:

a. tutte le firme;

b. il deposito di tutti gli strumenti di ratifica, accettazione, approvazione o adesione;

c. ogni data di entrata in vigore della presente Convenzione in base agli articoli 36 e 37;

d. ogni dichiarazione fatta in base all'articolo 40 o ogni riserve fatte in conformità all'articolo 42;

e. ogni altro atto, notifica o comunicazione relativa alla presente Convenzione.

In fede i sottoscritti, debitamente autorizzati a tal fine, hanno firmato la presente Convenzione .

Fatta a Budapest, il 23 novembre 2001, in inglese e francese, entrambi i testi egualmente autentici, in unica copia che dovrà essere depositata negli archivi del Consiglio d'Europa. Il Segretariato Generale del Consiglio d'Europa dovrà trasmettere copia certificata ad ogni Stato membro del Consiglio d'Europa, agli Stati non membri che hanno partecipato all'elaborazione della presente Convenzione e ad ogni Stato invitato ad aderirvi.

€ 4,40