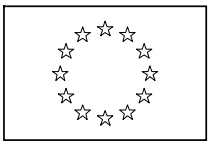

COMMISSIONE DELLE COMUNITÀ EUROPEE

Bruxelles, 19.04.2002
COM(2002)173 definitivo

2002/0086 (CNS)

Proposta di

DECISIONE-QUADRO DEL CONSIGLIO

relativa agli attacchi contro i sistemi di informazione

(presentata dalla Commissione)

RELAZIONE

1. INTRODUZIONE

Le reti elettroniche di comunicazione e i sistemi di informazione costituiscono al giorno d'oggi una parte essenziale della vita quotidiana dei cittadini dell'UE e sono fondamentali per il successo dell'economia dell'UE. Le reti ed i sistemi di informazione stanno convergendo e divenendo sempre più interconnessi. Tale evoluzione, nonostante i suoi vari ed ovvi benefici, ha anche portato con sé l'inquietante minaccia di attacchi intenzionali ai sistemi d'informazione. Tali attacchi possono assumere una grande varietà di forme, tra cui l'accesso illecito, la diffusione di codici "maligni" e gli attacchi finalizzati al diniego di servizio ("denial of service"). Un attacco può essere lanciato da qualsiasi posto al mondo, verso qualsiasi posto al mondo, e in qualsiasi momento. Nel futuro potrebbero verificarsi nuove, inaspettate forme di attacco.

Gli attacchi contro i sistemi d'informazione costituiscono una minaccia per la creazione di una società dell'informazione più sicura e di uno spazio di libertà, sicurezza e giustizia, e richiedono pertanto una risposta a livello di Unione europea. La presente proposta di decisione quadro relativa al ravvicinamento delle normative penali nel settore degli attacchi a sistemi d'informazione costituisce parte del contributo della Commissione a tale risposta.

1.1. Tipologie di attacchi ai sistemi d'informazione

L'espressione "sistemi d'informazione" viene qui usata deliberatamente nel suo senso più ampio, nel riconoscimento della convergenza tra reti elettroniche di comunicazione ed i vari sistemi che esse connettono. Ai fini della presente proposta, i sistemi d'informazione comprendono quindi personal computer "stand-alone", personal organiser digitali, telefoni cellulari, intranet, extranet e, ovviamente, le reti, i server e le altre infrastrutture di Internet.

Nella sua comunicazione "Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo"[1], la Commissione ha proposto le seguenti descrizioni delle minacce ai sistemi d'informazione:

a) **Accesso non autorizzato a sistemi d'informazione**. Vi rientra anche la nozione di "**hacking**". Per "hacking" s'intende il fatto di ottenere l'accesso non autorizzato ad un computer o ad una rete di computer. Si può intraprendere in vari modi, che vanno dal semplice sfruttamento di informazioni interne agli attacchi brutali e all'intercettazione di *password*. Ha spesso - ma non sempre - finalità dolose miranti a copiare, modificare o distruggere dati. Una delle finalità dell'accesso non autorizzato può essere il danneggiamento intenzionale di siti web o l'accesso senza pagare a servizi protetti da un accesso condizionato.

b) **Interruzione del funzionamento dei sistemi d'informazione.** Esistono svariati modi per interrompere il funzionamento dei sistemi d'informazione attraverso attacchi dolosi. Uno dei modi più conosciuti per bloccare o rallentare i servizi offerti da Internet è l'attacco "**denial of service**" (**diniego di servizio)** (DoS). In un certo senso questo tipo di attacco è simile a quello che consiste nel saturare gli apparecchi

[1] Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni "Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo" del 6.6.2001. COM (2001) 298 def.

fax con messaggi lunghi e ripetuti. Gli attacchi di tipo "denial of service" consistono nel tentativo di sovraccaricare i server web o i fornitori di servizi Internet (ISP) con messaggi generati automaticamente. Altri tipi di attacchi possono essere rivolti contro i server dei nomi di dominio (DNS) e contro i "router". Gli attacchi miranti ad interrompere il funzionamento dei sistemi sono risultati dannosi per alcuni siti web di alto profilo come i portali. Alcuni studi hanno calcolato che un recente attacco ha cagionato un danno di varie centinaia di milioni di euro, oltre al danno immateriale alla reputazione. Le aziende fanno sempre più affidamento sui propri siti web per i loro affari e quelle che dipendono dal web per le forniture "just in time" sono particolarmente vulnerabili.

c) **Esecuzione di software "maligni" (malicious software) che modificano o distruggono i dati.** Il tipo di software "maligno" più conosciuto è il virus. Tra gli esempi più tristemente noti si annoverano i virus "I Love You", "Melissa" e "Kournikova". Circa l'11 % degli utenti europei ha contratto un virus nel proprio personal computer (PC) a casa. Esistono altri tipi di software "maligno". Alcuni danneggiano il PC stesso, mentre altri usano il PC per attaccare altri componenti collegati in rete. Alcuni programmi (spesso chiamati *logic bombs* o "bombe logiche") possono rimanere inerti fino al momento in cui vengono innescati da un determinato evento, come ad esempio una data, al cui verificarsi possono cagionare danni notevoli alterando o distruggendo dati. Altri programmi sono in apparenza benigni ma, una volta attivati, lanciano un attacco distruttivo (spesso chiamati "cavalli di Troia"). Un'altra variante è costituita da quei programmi (detti *worms*, "bachi") che non infettano gli altri programmi ma si autoduplicano in copie che, riproducendosi a loro volta, finiscono col saturare il sistema.

d) **Intercettazione di comunicazioni**. L'intercettazione dolosa delle comunicazioni compromette la riservatezza e i requisiti d'integrità per gli utenti. Viene spesso chiamata "*sniffing*".

e) **Falsa rappresentazione della propria identità**. I sistemi d'informazione offrono nuove opportunità per operare false rappresentazioni della propria identità e frodi. L'usurpazione dell'identità di un soggetto su Internet ed il suo uso a fini dolosi è spesso chiamata "*spoofing*".

1.2. La natura della minaccia

Esiste un'esigenza evidente di raccogliere informazioni affidabili sulla dimensione e la natura degli attacchi ai sistemi d'informazione.

Alcuni dei più gravi episodi di attacchi ai sistemi d'informazione sono diretti contro operatori o fornitori di servizi di reti elettroniche di comunicazione o contro società di commercio elettronico. Anche settori più tradizionali possono però essere seriamente coinvolti considerata la sempre maggiore interconnessione nell'area delle comunicazioni moderne: industrie manifatturiere; industrie di servizi; ospedali; altre organizzazioni nel settore pubblico e gli stessi governi. Ma le vittime degli attacchi non sono solo organizzazioni; vi possono essere effetti molto diretti, gravi e dannosi anche sui singoli individui. L'onere economico che alcuni di questi attacchi comportano per organismi pubblici, società private e singoli individui indistintamente è considerevole e rischia di rendere i sistemi d'informazione più costosi e meno alla portata degli utenti.

I tipi di attacchi sopra descritti sono spesso portati avanti da soggetti che agiscono individualmente, a volte minori che forse non valutano appieno la gravità delle proprie azioni. Tuttavia, il livello di sofisticazione e di ambizione degli attacchi potrebbe accrescersi. Vi è una crescente ed inquietante preoccupazione che organizzazioni criminali possano usare le reti di comunicazione per sferrare attacchi contro i sistemi d'informazione per i propri scopi. I gruppi organizzati di *hacking* specializzati nell'accesso non autorizzato e la deturpazione di siti web sono sempre più attivi a livello mondiale. Tra gli esempi si possono citare i Brazilian Silver Lords ed i Pakistan Gforce, che tentano di estorcere denaro alle loro vittime, offrendo loro assistenza dopo aver effettuato un'intrusione non autorizzata nei loro sistemi d'informazione. L'arresto di grandi gruppi di *hacker* è indice del fatto che l'accesso non autorizzato potrebbe diventare sempre più un fenomeno di criminalità organizzata. Recentemente si sono verificati attacchi sofisticati ed organizzati contro la proprietà intellettuale nonché tentativi di sottrarre importi notevoli dai servizi bancari[2].

Anche le infiltrazioni nei dispositivi di sicurezza delle banche dati di operatori del commercio elettronico attraverso le quali si può ottenere l'accesso alle informazioni relative ai clienti, tra cui il loro numero di carta di credito, costituiscono un motivo di preoccupazione. Questi attacchi si traducono in maggiori opportunità di frodi nei pagamenti ed in ogni caso costringono gli operatori bancari ad annullare e riemettere migliaia di carte. Un'ulteriore conseguenza è il danno intangibile che subiscono la reputazione del commerciante e la fiducia del consumatore nel commercio elettronico. Delle misure preventive, quali requisiti minimi di sicurezza per i commercianti on line che accettano carte di pagamento, sono in discussione nel quadro del piano d'azione[3] per prevenire le frodi e le falsificazioni dei mezzi di pagamento diversi dai contanti.

La presente proposta fa anche parte del contributo della Commissione alla risposta alla minaccia di attacchi terroristici ai danni di sistemi di informazione vitali all'interno dell'Unione europea. Essa fa da complemento alle proposte della Commissione relative alla sostituzione dell'estradizione all'interno dell'Unione europea con un mandato d'arresto europeo[4] ed al ravvicinamento delle legislazioni relative al terrorismo[5], su cui si è raggiunto un accordo a livello politico in occasione del Consiglio europeo di Laeken del 14/15 dicembre 2001. Presi tutti insieme, questi strumenti assicureranno la presenza di norme penali efficaci per affrontare il ciberterrorismo in ogni Stato membro dell'Unione europea, e miglioreranno la cooperazione internazionale contro il terrorismo.

La proposta non si riferisce solo ad atti rivolti contro gli Stati membri, ma si applica altresì a condotte poste in essere nel territorio dell'Unione europea e però dirette contro sistemi di informazione che si trovano nel territorio di paesi terzi. Ciò riflette l'impegno della Commissione ad affrontare gli attacchi contro sistemi di informazione a livello sia globale che di Unione europea.

---

2 Secondo un'indagine pubblicata dalla Communications Management Association (CMA), sono state vittime di attacchi di "hacking" un terzo delle grandi società del Regno Unito e delle organizzazioni del settore pubblico, compresi uffici statali, che hanno causato danni che vanno dall'infiltrazione nei conti bancari di società fino al furto d'informazioni. Si veda l'indagine sul sito http:/www.cma.org.

3 Comunicazione della Commissione "Prevenire le frodi e le falsificazioni dei mezzi di pagamento diversi dai contanti", COM (2001) 11 def.. Adottata dalla Commissione il 9.2.2001.

4 Proposta di decisione quadro del Consiglio relativa al mandato d'arresto europeo e alle procedure di consegna fra gli Stati membri. COM(2001) 522 def. Adottata dalla Commissione il 19.9.2001.

5 Proposta di decisione quadro del Consiglio sulla lotta contro il terrorismo, COM(2001) 521 def. Adottata dalla Commissione il 19.9.2001.

Infatti, vi sono già state diverse occasioni di recente in cui le tensioni nelle relazioni internazionali hanno portato ad un'ondata di attacchi contro sistemi di informazione, che spesso hanno compreso attacchi a siti web. Attacchi più gravi potrebbero comportare non solo danni finanziari gravi ma, in alcuni casi, potrebbero addirittura comportare la perdita di vite umane (ad esempio sistemi ospedalieri, sistemi di controllo del traffico aereo, ecc.). L'importanza che gli Stati membri attribuiscono a questo rischio è dimostrata dalla priorità conferita alle varie iniziative relative alla protezione delle infrastrutture critiche. Ad esempio, il programma UE Tecnologie della società dell'informazione (TSI)[6] ha istituito, in collaborazione con il Dipartimento di Stato americano, una task force comune UE/USA per la protezione dell'infrastruttura critica[7].

1.3. La necessità di informazioni accurate e di statistiche

Esistono poche statistiche affidabili sulla dimensione globale del fenomeno della criminalità informatica. Il numero delle intrusioni individuate e denunciate fino ad oggi probabilmente non rappresenta appieno l'ampiezza del problema. Secondo un'indagine fatta negli Stati Uniti[8], nel 1999 solo il 32% degli intervistati che avevano subito un'intrusione nel proprio computer durante l'anno precedente l'aveva denunciata ai fini dell'azione penale. E questo costituiva un miglioramento rispetto agli anni precedenti in cui solo il 17% aveva sporto denuncia. Sono state avanzate numerose ragioni per giustificare la mancata denuncia. A causa della conoscenza ed esperienza limitata degli amministratori e degli utenti del sistema, molte intrusioni non vengono individuate. Inoltre, molte aziende non denunciano volentieri gli abusi informatici per evitare la cattiva pubblicità nonché l'esposizione ad attacchi in futuro. Molte forze dell'ordine ancora non conservano statistiche sull'uso dei computer e sui sistemi di comunicazione coinvolti in questi ed altri reati[9]. Le autorità preposte ad assicurare il rispetto della legge non sono sufficientemente addestrate ad individuare, identificare, ed investigare sui reati informatici. Ciononostante, l'Unione europea ha cominciato ad affrontare questa problematica attraverso la raccolta di alcune cifre relative agli attacchi contro sistemi di informazione. In uno Stato membro, è stato calcolato che gli attacchi a sistemi di informazione nel 1999 sono stati tra i 30 e i 40 mila, mentre sono state registrate non più di 105 denunce formali in questo campo. In effetti, nel 1999, sette Stati membri hanno registrato un totale di sole 1844 denunce formali relative a reati contro sistemi di informazione e dati informatici. Eppure, questa cifra è doppia rispetto a quella registrata nel 1998, in cui in quei sette Stati membri erano stati registrati solo 972 casi[10].

---

6 Il programma TSI viene gestito dalla Commissione europea. Fa parte del 5° Programma quadro, che va dal 1998 al 2002. Maggiori informazioni sono disponibili sul sito http://www.cordis.lu/ist.

7 Sotto gli auspici del gruppo consultivo comune dell'accordo di cooperazione CE/USA in materia tecnologica.

8 Il Computer Security Institute (CSI) ed il Federal Bureau of Investigation (FBI) producono un'indagine annuale sulla criminalità e sulla sicurezza informatica ("Computer Crime and Security Survey"), che viene pubblicato agli inizi di ogni anno. Il sito del CSI ed ulteriori dettagli sull'inchiesta si possono trovare su **www. gocsi.com**

9 Il Ministero degli Interni italiano ha recentemente pubblicato delle statistiche sulle sue attività operative volte a contrastare la criminalità informatica nel 1999 e 2000 (si veda http://www.mininterno.it/dip_ps/dcpsffp/index.htm). Le denunce ufficiali relative a casi di "hacking" nel 2000 sono 98, quattro volte la cifra riportata per il 1999, in cui sono stati registrati ufficialmente solo 21 casi.

10 Documento del Consiglio 8123/01 ENFOPOL 38. Disponibile sul sito web del Consiglio http://db.consilium.eu.int/jai

Inoltre, una recente inchiesta[11] riporta che il 13 per cento delle aziende che erano state vittima di reati contro il patrimonio hanno dichiarato che uno dei reati era stato un reato informatico. L'inchiesta ha anche evidenziato una preoccupazione crescente nei confronti della criminalità informatica, con il 43 per cento degli intervistati convinti che la criminalità informatica costituirà un rischio del futuro. Un altro studio è giunto alla conclusione che *hackers* e virus costituiscono attualmente la maggiore minaccia di criminalità informatica per le organizzazioni, evidenziando come i principali autori di reati siano *hackers* (45 per cento), ex dipendenti (13 per cento), criminalità organizzata (13 per cento) e dipendenti attuali (11 per cento)[12]. Queste cifre probabilmente continueranno a crescere man mano che aumenterà l'uso di sistemi di informazione e dell'interconnettività, e che aumenterà la disponibilità a denunciare questi attacchi. Ma è evidente che sono necessarie misure urgenti per produrre uno strumento statistico da utilizzarsi in tutti gli Stati membri in modo tale che i reati informatici nell'Unione europea possano essere misurati quantitativamente e qualitativamente. Il punto di partenza per un'analisi del genere è una definizione comune a livello di Unione europea dei reati commessi negli attacchi ai sistemi di informazione.

1.4. Il contesto delle politiche dell'Unione europea

In questo contesto il Consiglio europeo, riunito a Lisbona nel marzo del 2000, ha sottolineato l'importanza della transizione verso un'economia competitiva, dinamica e basata sulla conoscenza ed ha invitato il Consiglio e la Commissione ad elaborare un piano d'azione globale per l'Europa telematica (Piano d'azione *e*Europe) per trarre il massimo vantaggio da questa opportunità.[13] Il suddetto piano d'azione, preparato dalla Commissione e dal Consiglio, e approvato in occasione della riunione del Consiglio europeo a Feira nel giugno 2000, contempla azioni volte a promuovere la sicurezza delle reti e l'adozione di una strategia coordinata e coerente per far fronte alla criminalità informatica entro la fine dell'anno 2002.

La Commissione ha pubblicato, come parte del suo contributo a questo impegno contro la criminalità telematica, una comunicazione intitolata "Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica"[14]. Tale comunicazione proponeva un approccio bilanciato alla soluzione dei problemi di criminalità telematica, tenendo pieno conto delle opinioni di tutte le parti interessate, compresi gli organismi preposti all'applicazione della legge, i prestatori di servizi Internet, gli operatori delle reti, gli altri gruppi industriali, i rappresentanti dei consumatori, le autorità garanti della protezione dei dati e i gruppi che si occupano della tutela della vita privata. La comunicazione proponeva una serie di iniziative sia legislative che non legislative.

Un esempio importante di azione attualmente in corso è quella nell'ambito del programma IDA, in cui gli Stati membri e la Commissione già stanno lavorando su una strategia comune di sicurezza e stanno ponendo in essere una rete sicura per lo scambio d'informazioni amministrative.

Una delle questioni chiave affrontate dalla comunicazione era l'esigenza di un'azione efficace per fare fronte alle minacce contro l'autenticità, l'integrità, la riservatezza e la disponibilità dei sistemi e delle reti di informazione. A livello di legislazione comunitaria, già molto è stato

---

11 "European Economic Crime Survey 2001", PricewaterhouseCoopers 2001 (http://www.pwcglobal.com)

12 "The Cybercrime Survey 2001", Confederation of British Industry (si veda http://www.cbi.org.uk)

13 Conclusioni della presidenza del Consiglio europeo di Lisbona tenuto il 23 e 24 marzo 2000, reperibili all'indirizzo: http://ue.eu.int/en/Info/eurocouncil/index.htm.

14 COM (2000) 890 def.

fatto. Esistono già diverse misure legislative a livello comunitario che comportano specifiche implicazioni per la sicurezza delle reti e dell'informazione.

La presente decisione quadro completa quanto già realizzato nell'ambito della legislazione comunitaria per proteggere i sistemi d'informazione, come ad esempio le direttive 95/46/CE, 97/66/CE e 98/84/CE sulla tutela giuridica dei sistemi ad accesso condizionato e dei sistemi di accesso condizionato. In particolare, il quadro europeo di protezione delle telecomunicazioni e dei dati (direttive 95/46/CE e 97/66/CE[15]) contiene disposizioni volte ad assicurarsi che i fornitori di servizi di telecomunicazione aperti al pubblico adottino le misure tecniche ed organizzative adeguate a preservare la sicurezza e la riservatezza dei propri servizi e che tali misure garantiscano un livello di sicurezza adeguato al rischio prospettato.

Uno dei modi più importanti ed efficaci di affrontare questi problemi è costituito dalla prevenzione e dalla formazione. La comunicazione evidenziava l'importanza della disponibilità, dello sviluppo, dell'applicazione e dell'uso effettivo delle tecnologie di prevenzione. Essa sottolineava la necessità di innalzare il livello di consapevolezza dei rischi posti dalla criminalità informatica, promuovere le migliori pratiche per la sicurezza informatica (IT), sviluppare strumenti e procedure efficaci per contrastare la criminalità informatica ed incoraggiare l'ulteriore sviluppo di meccanismi di preallarme e di gestione di crisi. Il programma UE Tecnologie della società dell'informazione (TSI)[16] fornisce un quadro per sviluppare le capacità e tecnologie necessarie per comprendere ed affrontare le sfide emergenti in materia di criminalità informatica.

Più di recente, il Consiglio europeo riunito a Stoccolma il 23-24 marzo ha riconosciuto l'esigenza di azioni ulteriori nel settore della sicurezza delle reti e dell'informazione ed ha concluso che *"il Consiglio svilupperà insieme alla Commissione una strategia globale per la sicurezza delle reti elettroniche, comprensiva di azioni concrete di attuazione. Tale strategia dovrebbe essere presentata in tempo per il Consiglio europeo di Göteborg."* La Commissione ha risposto a questo appello con la sua comunicazione "Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo"[17]. Tale comunicazione analizza i problemi attuali della sicurezza delle reti e delinea un progetto di azione strategica in questo settore. È stata seguita da una risoluzione del Consiglio del 6 dicembre 2001 relativa ad un approccio comune e ad azioni specifiche nel settore della sicurezza delle reti e dell'informazione. Queste iniziative non sono da sole sufficienti a dare tutte le risposte necessarie agli attacchi gravi ai sistemi di informazione. Entrambe le citate comunicazioni della Commissione riconoscevano anche che esiste una necessità urgente di ravvicinamento del diritto penale sostanziale all'interno dell'Unione europea nel settore degli attacchi ai sistemi di informazione. Ciò riflette le conclusioni del vertice del Consiglio europeo di Tampere nell'ottobre 1999[18] che fanno rientrare la criminalità ad alta tecnologia nel ristretto elenco dei settori su cui si debbono incentrare gli sforzi intesi a concordare definizioni, incriminazioni e sanzioni comuni, ed è stato inserito nella raccomandazione 7 della strategia dell'Unione europea per l'inizio del nuovo millennio in materia di prevenzione e controllo della criminalità organizzata adottata dal Consiglio GAI del marzo 2000.[19] La presente proposta di decisione quadro fa parte anche del programma di lavoro della

---

15 GU L. 281 del 23.11.1995, pag. 31-50, GU L 024 del 30.01.1998, pag. 1-8.

16 Il programma TSI viene gestito dalla Commissione europea. Fa parte del 5° Programma quadro, che va dal 1998 al 2002. Maggiori informazioni sono disponibili sul sito http://www.cordis.lu/ist.

17 COM (2001) 298 def. del 6 giugno 2001.

18 http://db.consilium.eu.int/en/Info/eurocouncil/index.htm.

19 Prevenzione e controllo della criminalità organizzata. Strategia dell'Unione europea per l'inizio del nuovo millennio (GU 2000 C 124 del 3.5.2000).

Commissione per l'anno 2001[20] e del quadro di controllo per l'esame dei progressi compiuti nella creazione di uno spazio di libertà sicurezza e giustizia, elaborato dalla Commissione il 30 ottobre 2001[21].

1.5. L'esigenza di un ravvicinamento delle normative penali

Le normative degli Stati membri in questo settore contengono lacune e differenze significative che rischiano di ostacolare la lotta contro la criminalità organizzata ed il terrorismo, nonché contro gli attacchi gravi perpetrati da singoli ai danni di sistemi di informazione. Un ravvicinamento del diritto sostanziale nel settore dei reati ad alta tecnologia farebbe sì che le normative nazionali fossero abbastanza esaurienti da permettere che tutte le forme di attacchi gravi ai danni di sistemi di informazione possano essere oggetto di indagini condotte con le tecniche ed i metodi usati nelle indagini penali. Gli autori di siffatti reati devono essere individuati e perseguiti in giustizia e i giudici devono avere a disposizione pene adeguate e proporzionate. Ciò costituirà un forte deterrente per coloro che hanno intenzione di perpetrare attacchi contro sistemi di informazione.

Inoltre, le lacune e le differenze esistenti potrebbero costituire un ostacolo ad un'efficiente cooperazione giudiziaria e di polizia nel settore degli attacchi a sistemi di informazione. Gli attacchi ai sistemi di informazione potrebbero spesso avere natura transnazionale, richiedendo pertanto una cooperazione internazionale giudiziaria e di polizia. Il ravvicinamento delle legislazioni migliorerà tale cooperazione, facendo sì che sia soddisfatta la condizione della doppia incriminazione (secondo cui una condotta deve costituire reato in entrambi i paesi affinché ci si possa fornire reciproca assistenza giudiziaria nel corso di un'indagine penale). Questo risulterà utile agli Stati membri dell'UE nella cooperazione tra di loro e favorirà anche la cooperazione tra Stati membri dell'UE e paesi terzi (purché esista, in questo caso, un adeguato accordo di reciproca assistenza giudiziaria).

Vi è altresì l'esigenza di completare gli strumenti esistenti a livello di Unione europea. La decisione quadro sul mandato d'arresto europeo[22], l'allegato alla convenzione Europol[23] e la decisione del Consiglio che ha istituito Eurojust[24] contengono riferimenti alla criminalità informatica che devono essere definiti con maggiore precisione. Ai fini di tali strumenti, la criminalità informatica dev'essere intesa come comprensiva degli attacchi a sistemi di informazione quali definiti nella presente decisione quadro, che fornirà un livello molto più elevato di ravvicinamento degli elementi costitutivi di tali reati. La presente decisione quadro completa anche la decisione quadro sulla lotta al terrorismo[25] che si applica ad azioni terroristiche che cagionino danni sostanziali ad un'infrastruttura, quale anche un sistema di informazione, suscettibili di porre in pericolo la vita umana o di generare ingenti perdite economiche.

---

20 http://europa.eu.int/comm/off/work_programme/index_en.htm

21 http://europa.eu.int/comm/dgs/justice_home; COM (2001) 628 def. del 30.10.2001

22 GU C... pag...

23 Atto del Consiglio, del 26 luglio 1995, che stabilisce la convenzione basata sull'articolo K.3 del trattato sull'Unione europea che istituisce un ufficio europeo di polizia (Convenzione Europol), GU C 316 del 27.11.1995, pag. 1.

24 GU C..., pag...

25 GU C..., pag...

1.6. Ambito e finalità della proposta di decisione quadro

Gli obiettivi della presente decisione quadro del Consiglio sono appunto quelli di ravvicinare le legislazioni penali nel settore degli attacchi a sistemi di informazione, e di garantire la massima cooperazione giudiziaria e di polizia possibile nel campo dei reati legati agli attacchi contro sistemi di informazione. Inoltre, questa proposta costituisce un contributo all'impegno dell'Unione europea nella lotta contro la criminalità organizzata ed il terrorismo. La presente decisione quadro non mira ad imporre agli Stati membri di qualificare come reati condotte di scarsa gravità o banali.

Dall'articolo 47 del trattato sull'Unione europea emerge chiaramente che la presente decisione quadro non pregiudica l'applicazione del diritto comunitario. In particolare, essa fa salvi i diritti e gli obblighi in materia di tutela della vita privata o di protezione dei dati contemplati da atti normativi comunitari, quali le direttive 95/46/CE e 97/66/CE. La decisione quadro non mira a obbligare gli Stati membri a qualificare come reato la violazione delle regole d'accesso a - o di diffusione di - dati personali, norme relative alla segretezza delle comunicazioni, norme sulla sicurezza del trattamento dei dati personali, norme relative alla firma elettronica[26] o norme relative ai diritti di proprietà intellettuale, e fa salva l'applicazione della direttiva 98/84/CE sulla tutela giuridica dei sistemi ad accesso condizionato e dei sistemi di accesso condizionato[27]. Si tratta di questioni importanti, ma che sono già contemplate dalla legislazione comunitaria esistente. Qualsiasi ravvicinamento della legislazione penale in questi campi, quali la protezione dei dati personali, la remunerazione dei prestatori di servizi ad accesso condizionato o la proprietà intellettuale, deve quindi essere considerato nel quadro della legislazione comunitaria piuttosto che in quello del titolo VI del trattato UE. Per questi motivi, la presente decisione quadro si limita ad affrontare le condotte descritte ai punti da a) a c) della sezione 1.1.

Un'azione legislativa a livello di Unione europea deve anche tenere conto degli sviluppi in altre sedi internazionali. Nel contesto del ravvicinamento del diritto penale sostanziale in materia di attacchi a sistemi d'informazione, il Consiglio d'Europa è attualmente il più avanzato. Il Consiglio d'Europa ha cominciato a preparare una convenzione internazionale sulla criminalità telematica (cibercriminalità) nel febbraio 1997, e tale convenzione è stata formalmente adottata ed aperta alle firme nel novembre 2001[28]. La convenzione si pone come obiettivo quello di ravvicinare una serie di reati, tra cui reati contro la riservatezza, l'integrità e la disponibilità di sistemi e dati informatici. La presente decisione quadro è concepita per essere coerente con l'approccio adottato nella convenzione del Consiglio d'Europa per questi reati.

Durante le discussioni in seno al G8 sulla criminalità tecnologica, sono state individuate due principali categorie di minacce. Innanzitutto, le minacce contro le infrastrutture informatiche, che riguardano le operazioni tese ad interrompere, rifiutare, corrompere o distruggere le informazioni inserite nei computer e nelle reti di computer, o gli stessi computer e reti. In secondo luogo, le minacce perpetrate a mezzo di computer, che riguardano attività dolose come la frode, il riciclaggio di denaro sporco, la pornografia infantile, la violazione dei diritti

---

26 Direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche, GU L 13 del 19.01.2000, pag.12.

27 GU L. 320 del 28.11.1998, pag.54-57.

28 Il testo è disponibile in Internet, in due lingue,
francese: http://conventions.coe.int/treaty/fr/projets/cybercrime.htm.
ed inglese: http://conventions.coe.int/treaty/en/projets/cybercrime.htm.

di proprietà intellettuale e il traffico di droga, che sono facilitati dall'uso di computer. La presente proposta si occupa della prima categoria di minacce.

Il ravvicinamento delle legislazioni a livello di UE deve tenere conto degli sviluppi intervenuti nelle sedi internazionali e dev'essere coerente con le attuali politiche comunitarie. La presente proposta intende anche introdurre, all'interno dell'Unione europea, un grado di ravvicinamento maggiore di quello che è stato possibile raggiungere negli altri consessi internazionali.

2. BASE GIURIDICA

L'obiettivo della creazione di uno spazio di libertà, sicurezza e giustizia deve essere conseguito prevenendo e reprimendo la criminalità, organizzata o di altro tipo, in particolare il terrorismo, mediante una più stretta cooperazione tra autorità giudiziarie e altre autorità competenti negli Stati membri, nonché mediante il ravvicinamento delle normative degli Stati membri in materia penale. La presente proposta di decisione quadro mira pertanto a ravvicinare le disposizioni legislative e regolamentari degli Stati membri nel settore della cooperazione giudiziaria e di polizia in materia penale. Essa riguarda la fissazione di "norme minime relative agli elementi costitutivi dei reati", in particolare, e sostanzialmente, nel campo della criminalità organizzata e del terrorismo. Essa comporta anche la "garanzia della compatibilità delle normative applicabili negli Stati membri" per facilitare ed accelerare la cooperazione tra autorità giudiziarie. La base giuridica indicata nel preambolo della proposta è quindi costituita dagli articoli 29, 30, lettera a), 31 e 34, paragrafo 2, lettera b) del trattato sull'Unione europea. La proposta non ha conseguenze finanziarie per il bilancio delle Comunità europee.

3. LA DECISIONE QUADRO: ARTICOLI

Articolo 1 - Ambito d'applicazione e finalità

Questo articolo afferma esplicitamente che la finalità della decisione quadro è quella del ravvicinamento delle normative penali nel settore degli attacchi gravi a sistemi di informazione, in particolare per dare un contributo alla lotta contro la criminalità organizzata ed il terrorismo e, in tale modo, assicurare la più ampia cooperazione giudiziaria possibile nel settore dei reati collegati ad attacchi contro sistemi d'informazione. In conformità con l'articolo 47 del trattato sull'Unione europea, la presente decisione quadro fa anche salva l'applicazione del diritto comunitario. In particolare ciò comprende i diritti e le obbligazioni in materia di tutela della vita privata o di protezione dei dati di cui alle direttive 95/46/CE e 97/66/CE. La presente decisione quadro non è intesa ad esigere che gli Stati penalizzino le violazioni delle norme sull'accesso ai dati personali o sulla loro divulgazione, sulla segretezza delle comunicazioni, sulla sicurezza del trattamento dei dati personali, sulla firma elettronica[29] o la violazione delle norme che tutelano la proprietà intellettuale e fa salva l'applicazione della direttiva 98/84/CE sulla tutela giuridica dei servizi ad accesso condizionato e dei servizi di accesso condizionato[30].

---

[29] Direttiva 1999/93/CE del Parlamento europeo e del Consiglio del 13 dicembre 1999 relativa ad un quadro comunitario per le firme elettroniche, GU L 13 del 19.01.2000, pag.12.

[30] GU L 320 del 28.11.1998, pagg. 54-57.

La presente decisione quadro non intende esigere dagli Stati membri la penalizzazione di condotte di scarsa gravità o banali. Gli articoli 3 e 4 definiscono i criteri che devono essere soddisfatti per penalizzare un'azione. Questi criteri sono coerenti con la deroga e le possibilità di riserve contenute nel progetto di convenzione del Consiglio d'Europa sulla criminalità telematica.

Tutti i reati contemplati nella presente decisione quadro devono essere stati commessi intenzionalmente. Il termine "intenzionale" è esplicitamente adoperato negli articoli 3, 4 e 5. Questa nozione dev'essere interpretata secondo i normali principi di diritto penale che disciplinano il dolo negli Stati membri. Pertanto, la decisione quadro non richiede che siano considerate reato le condotte connotate da negligenza grave o altro tipo di colpa, ma non da un'intenzione in quanto tale. È sufficiente l'intenzione generica di accedere illegalmente o di interferire con sistemi di informazione, senza bisogno di provare che l'intenzione si rivolgeva ad uno specifico sistema di informazione.

Articolo 2 - Definizioni

La proposta decisione quadro del Consiglio contiene la seguenti definizioni:

a) *"reti di comunicazione elettronica"*. Questa definizione è la stessa di quella adottata dal Consiglio e dal Parlamento europeo il 14 febbraio 2002 nella direttiva che istituisce un quadro normativo comune per le reti e i servizi di comunicazione elettronica[31].

b) *"computer"*. Questa definizione si basa sull'articolo 1 della convenzione internazionale sulla criminalità telematica ("cibercriminalità"). Nella definizione rientrano anche ad esempio, personal computer "stand-alone", *personal organiser* digitali, *set-top-box* digitali, videoregistratori personali e telefoni cellulari (purché abbiano qualche funzione di trattamento di dati, ad esempio i telefoni WAP e di terza generazione), che non rientrerebbero nella sola definizione di reti di comunicazione elettronica.

c) *"dati informatici"*. Questa definizione è costruita a partire dalla definizione di dati dell'ISO[32]. Non è volta a designare anche oggetti fisici come i libri. Tuttavia, comprende i libri immagazzinati sotto forma di dati informatici (ad esempio, salvati in forma elettronica come un documento di trattamento di testi) oppure trasformati in dati informatici mediante uno scanner. Per questa ragione, la definizione chiarisce che i dati informatici devono essere stati "creati o tradotti in una forma" adatta al trattamento in un sistema di informazione o adatti a creare una funzione in un sistema di informazione.

d) *"sistema di informazione"*. La definizione di sistema di informazione è tratta, originariamente, da quella adottata dall'OCSE nel 1992 nelle sue linee guida per la sicurezza dei sistemi di informazione e poggia sulle definizioni che precedono relative alle reti di comunicazione elettronica, computer e dati informatici. Il termine è anche stato usato in strumenti normativi comunitari precedenti, quali la decisione del Consiglio del 31 marzo 1992 nel settore della sicurezza dei sistemi di

---

31 Per il testo definitivo si veda http://europa.eu.int/information_society/topics/telecoms/regulatory/new_rf/index_en.htm#reg

32 L'Organizzazione internazionale per la standardizzazione (ISO) è una federazione mondiale di organismi di normalizzazione nazionali di circa 100 paesi.

informazione e nella raccomandazione del Consiglio del 7 aprile 1995 su criteri comuni per la valutazione della sicurezza delle tecnologie d'informazione. La definizione si vuole neutra per quanto riguarda la tecnologia, e intesa a riflettere accuratamente il concetto di reti interconnesse e sistemi contenenti dati. Vi rientrano sia l'hardware che il software del sistema, ma non il contenuto dell'informazione stessa. Vi rientrano anche i sistemi "stand alone". Secondo la Commissione, è auspicabile estendere la tutela del diritto penale anche ai computer stand-alone e non limitarla ai soli sistemi interconnessi.

e) *"persona giuridica"*. Si tratta di una definizione standard presente in precedenti decisioni quadro del Consiglio.

f) *"persona autorizzata"* . Significa ogni persona che ha il diritto, per contratto o per legge, o il permesso legittimo di usare, gestire, controllare, collaudare, condurre ricerche scientifiche o comunque far funzionare un sistema di informazione e che agisce in conformità con tale diritto o permesso. Rientrano in questa nozione coloro che agiscono con il consenso legittimo di chi possiede tale esplicita autorizzazione. È particolarmente importante che le seguenti categorie di persone e di attività legittime non siano (nei limiti dei diritti, dei permessi e delle responsabilità della persona e nel rispetto della legislazione comunitaria in materia di protezione dei dati e segretezza delle comunicazioni) penalizzate al momento dell'attuazione della presente decisione quadro nelle legislazioni nazionali:

- azioni degli utenti abituali, sia per uso privato che professionale, compreso l'uso da parte di tali utenti di una cifratura per proteggere le proprie comunicazioni e i propri dati;
- decompilazione, entro i limiti di cui alla direttiva 91/250/CEE del 14 maggio 1991 relativa alla tutela giuridica dei programmi per elaboratore[33]
- azioni dei gestori, dei soggetti addetti al controllo e degli operatori delle reti e dei sistemi;
- azioni delle persone autorizzate a collaudare un sistema, sia che si tratti di personale interno alla società sia che si tratti di persone designate dall'esterno ed autorizzate a collaudare la sicurezza del sistema;
- ricerca scientifica legittima.

g) *"senza diritto"*. Si tratta di una definizione ampia, che lascia una certa flessibilità agli Stati membri nel decidere l'esatto ambito del reato. Ciononostante, per assistere gli Stati nell'attuazione della decisione quadro del Consiglio nel diritto nazionale, la Commissione ritiene necessario indicare che alcune attività non devono ricadere nell'ambito del reato. Non è possibile, e probabilmente neanche auspicabile, stilare un elenco esaustivo di esenzioni a livello di Unione europea. Ma l'espressione "senza diritto" prende come punto di partenza le definizioni precedenti in modo da escludere la condotta delle persone autorizzate. Inoltre, essa esclude qualsiasi altra condotta riconosciuta come lecita dal diritto nazionale, compresi i mezzi di difesa generici e altri tipi di precedenti riconosciuti nel diritto nazionale.

---

[33] GU L 122 del 17.05.1991, pag. 42- 46.

Articolo 3 - Attacco mediante accesso illecito a sistemi di informazione

Questa formulazione mira a descrivere il reato di accesso illecito a sistemi di informazione. In tale definizione rientra il concetto di "hacking" di un sistema di informazione. Gli Stati membri, nell'attuazione della presente decisione quadro nel diritto interno, sono liberi di escludere casi di scarsa gravità o banali dall'ambito del reato in questione.

Si richiede che tale condotta costituisca reato per la legislazione degli Stati membri solo nella misura in cui sia stata commessa:

i) contro qualsiasi parte di un sistema di informazione che sia sottoposta a misure specifiche di protezione; o

ii) con l'intenzione di cagionare un danno a persone fisiche o giuridiche; o

iii) con l'intenzione di procurare un vantaggio economico.

La Commissione non intende negare in alcun modo la rilevanza dell'uso di misure tecniche efficaci per proteggere i sistemi di informazione. Ciononostante, è purtroppo innegabile che un'alta proporzione di utenti si espone agli attacchi in quanto non dispone di una protezione tecnica adeguata o addirittura non dispone di alcuna protezione. Per scoraggiare gli attacchi contro tali utenti, occorre che la legislazione penale preveda come reato l'accesso illecito ai loro sistemi anche qualora tali sistemi non vi sia una adeguata protezione tecnica per gli stessi. Per questo motivo, e purché vi sia o l'intenzione di cagionare un danno o l'intenzione di procurare un vantaggio economico, non è richiesto, ai fini della sussistenza del reato, che siano state superate misure di protezione.

Articolo 4 - Interferenza illecita con sistemi di informazione

Rientra in questo reato la condotta intenzionale di chi, senza diritto, compie uno dei seguenti atti:

a) ostacolare gravemente o interrompere, senza diritto, il funzionamento di un sistema di informazione attraverso l'inserimento, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di dati informatici. Gli elementi dell'inserimento e della trasmissione di dati informatici si riferiscono specificamente al problema dei cosiddetti attacchi del tipo "diniego di servizio" in cui vi è un tentativo deliberato di saturare un sistema di informazione. Il reato contempla anche "l'interruzione" del funzionamento di un sistema di informazione, che potrebbe essere dedotto dall'espressione "ostacolare" ma è menzionato in modo esplicito per maggiore chiarezza. Gli altri elementi del reato (il danneggiamento, la cancellazione, il deterioramento, l'alterazione o la soppressione di dati informatici) si riferiscono specificamente al problema dei virus, e degli altri tipi di attacchi volti ad ostacolare o a interrompere il funzionamento del sistema di informazione stesso.

b) cancellare, deteriorare, alterare, sopprimere o rendere inaccessibili dati informatici contenuti in un sistema d'informazione, qualora questi atti vengano commessi con l'intenzione di cagionare un danno a persone fisiche o giuridiche. Questa definizione contempla gli attacchi di virus che mirano al contenuto (o ai dati informatici) contenuti in un sistema di informazione, nonché la corruzione di siti web.

La lettera a) usa i termini "ostacolare gravemente o interrompere" come elementi costituitivi del reato al fine di descrivere gli effetti di tali attacchi. Il significato della nozione di

"ostacolare gravemente" non è definito, in quanto tale impedimento può assumere diverse forme ed il suo grado può variare a seconda del tipo di attacco e delle capacità tecniche del sistema di informazione che viene attaccato. Ogni Stato membro determina autonomamente i criteri che devono essere soddisfatti perché un sistema possa considerarsi "gravemente ostacolato". Tuttavia, disturbi o interruzioni minime del funzionamento del sistema non dovrebbero essere considerate come sufficienti a superare la soglia della "gravità".

Come per il precedente reato, gli Stati membri, nell'attuazione della presente decisione quadro nel loro diritto interno, sono liberi di escludere dall'ambito del reato casi di scarsa gravità o banali.

Articolo 5 - Istigazione, favoreggiamento, complicità e tentativo

L'articolo 5, paragrafo 1, istituisce l'obbligo per gli Stati membri di provvedere a che l'istigazione, il favoreggiamento o la complicità intenzionali nei confronti di reati contro sistemi di informazione di cui agli articoli 3 e 4 siano puniti come reato.

L'articolo 5, paragrafo 2, riguarda specificamente il tentativo. Esso impone agli Stati membri di provvedere a che il tentativo di commettere uno dei reati contro sistemi di informazione di cui agli articoli 3 e 4 sia punito come reato.

Articolo 6 – Pene

Il paragrafo 1 richiede che gli Stati membri adottino le misure necessarie a fare sì che i reati di cui agli articoli da 3 a 5 siano punibili con pene effettive, proporzionate e dissuasive[34]. Gli Stati membri sono tenuti, in virtù di questo paragrafo, a prescrivere pene commisurate alla gravità del reato, tra cui condanne ad una pena detentiva non inferiore, nel massimo, ad un anno per i casi gravi. La nozione di casi gravi si deve intendere come volta ad escludere i casi in cui la condotta non abbia cagionato alcun danno né alcun profitto economico.

La pena massima di almeno un anno di detenzione nei casi gravi fa rientrare questi reati nel campo d'applicazione del mandato d'arresto europeo nonché di altri strumenti quali la decisione quadro del Consiglio del 26 giugno 2001[35] concernente il riciclaggio di denaro, l'individuazione, il rintracciamento, il congelamento o sequestro e la confisca degli strumenti e dei proventi di reato.

Conformemente alla natura di tutte le decisioni quadro, che sono vincolanti per gli Stati membri solo per quanto riguarda il risultato da ottenere, ma lasciano alla loro discrezionalità la scelta delle forme e dei mezzi, gli Stati membri conservano un certo grado di flessibilità, entro i limiti imposti dalla decisione quadro, nell'adattare la propria legislazione alle norme della stessa e nel determinare la severità delle pene applicabili, in particolare per quanto riguarda le circostanze aggravanti di cui all'articolo 7. La Commissione sottolinea che spetta agli Stati membri decidere i criteri da usare per determinare la gravità di un reato, sulla base dei rispettivi ordinamenti giuridici.

Le pene non devono sempre assumere la forma della detenzione in carcere. Il paragrafo 2 prevede la possibilità per gli Stati membri di imporre pene pecuniarie in aggiunta o in

---

[34] La formulazione è ripresa dalla sentenza della Corte di giustizia del 21 settembre 1989 nella causa 68/88, Racc.[1989] 2965.

[35] GU L 182 del 5.7.2001, pag.1.

sostituzione delle pene detentive, in conformità con le proprie tradizioni ed i propri ordinamenti giuridici.

Articolo 7 - Circostanze aggravanti

Questo articolo impone agli Stati membri di aumentare le pene di cui all'articolo 6 in presenza di alcune circostanze. La Commissione sottolinea che l'elenco delle circostanze aggravanti di cui al presente articolo lascia impregiudicata l'applicazione di altre circostanze aggravanti previste nella legislazione degli Stati membri. Questo elenco tiene conto delle circostanze aggravanti previste da disposizioni nazionali o da precedenti proposte di decisioni quadro della Commissione.

La pena detentiva non può essere inferiore, nel massimo, a quattro anni, qualora si verifichi una delle seguenti condizioni:

a) il reato è stato commesso nell'ambito di un'organizzazione criminale ai sensi dell'azione comune 98/733 GAI, a parte il livello di pena ivi previsto;

b) il reato ha cagionato, o ha dato origine a, ingenti perdite economiche dirette o indirette, danni corporali a persone fisiche o danni rilevanti ad una parte dell'infrastruttura critica di uno Stato membro; o

c) il reato ha procurato elevati proventi.

Gli Stati membri devono altresì provvedere affinché i reati di cui agli articoli 3, 4 e 5 siano punibili con pene detentive più severe di quelle previste all'articolo 6 qualora l'autore del reato sia stato condannato con sentenza definitiva in uno degli Stati membri dell'Unione per un tale reato.

Articolo 8 - Circostanze particolari

Questo articolo prevede delle circostanze in presenza delle quali uno Stato membro può decidere di ridurre le pene di cui agli articoli 6 e 7 qualora, a giudizio dell'autorità giudiziaria competente, l'autore abbia causato solo un danno di lieve entità.

Articolo 9 - Responsabilità delle persone giuridiche

In linea con l'approccio assunto in una serie di strumenti legislativi adottati a livello di Unione europea per contrastare diversi tipi di criminalità, è necessario anche prevedere la situazione in cui una persona giuridica sia coinvolta in attacchi contro sistemi di informazione. L'articolo 9 contiene pertanto disposizioni volte a fare sì che una persona giuridica possa essere ritenuta responsabile dei reati di cui agli articoli 3, 4 e 5, commessi a suo vantaggio da chiunque rivesta una posizione di preminenza, che agisca a titolo individuale o in quanto parte di un organo della persona giuridica. La nozione di responsabilità s'intende comprensiva di responsabilità civile e penale.

Inoltre, conformemente ad una prassi uniforme, il paragrafo 2 prevede che una persona giuridica possa essere ritenuta responsabile qualora la mancata supervisione o la mancata sorveglianza della persona che si trova nella posizione di esercitare la sorveglianza, ha reso possibile la commissione dei reati a vantaggio della persona giuridica. Il paragrafo 3 indica che l'avvio di un procedimento giudiziario contro una persona giuridica non preclude la possibilità di avviare parallelamente un procedimento giudiziario contro una persona fisica.

Articolo 10 - Sanzioni applicabili alle persone giuridiche

L'articolo 10 richiede la previsione di sanzioni per le persone giuridiche riconosciute responsabili per i reati di cui agli articoli 3, 4 e 5. L'articolo richiede sanzioni effettive, proporzionate e dissuasive per cui l'obbligo minimo è quello di applicare sanzioni pecuniarie di natura penale o non. Sono anche indicate altre sanzioni che potrebbero tipicamente applicarsi a persone giuridiche.

Articolo 11 - Giurisdizione

La natura internazionale dei reati che comportano attacchi a sistemi di informazione fa sì che un risposta sul piano della legislazione penale richieda disposizioni procedurali sulla giurisdizione e sull'estradizione chiare e avanzate a livello di Unione europea, in modo da assicurare che gli autori di tali reati non sfuggano alla giustizia.

Il paragrafo 1 stabilisce alcuni criteri per attribuire alle autorità giudiziarie nazionali la competenza a perseguire ed investigare su casi relativi ai reati di cui alla presente decisione quadro. Uno Stato membro stabilisce la propria giurisdizione in tre situazioni:

a) qualora il reato sia commesso anche solo parzialmente sul suo territorio, a prescindere dallo status o dalla nazionalità dell'autore (principio di territorialità);

b) qualora l'autore del reato sia un cittadino di quello Stato (principio della personalità attiva) e il reato colpisca individui o gruppi di tale Stato. Gli Stati membri che non ne prevedano l'estradizione hanno la responsabilità di perseguire i propri cittadini che abbiano commesso il reato all'estero;

c) qualora il reato sia commesso a beneficio di una persona giuridica che ha la sua sede nel territorio di quello Stato membro.

Il paragrafo 2 mira a garantire che ogni Stato membro, quando stabilisce la propria giurisdizione sui reati in base al principio di territorialità di cui al paragrafo 1, lettera a), provveda a che vi rientrino i casi in cui:

a) l'autore commette il reato mentre è fisicamente presente sul suo territorio, indipendentemente dal fatto che il reato sia o meno perpetrato ai danni di un sistema di informazione che si trova sul suo territorio - ad esempio, una persona che, dal territorio dello Stato membro, ottenga un accesso illecito (hacking) ad un sistema di informazioni sito in un paese terzo - o

b) il reato è perpetrato ai danni di un sistema di informazioni situato nel suo territorio, indipendentemente dal fatto che l'autore del reato sia o meno fisicamente presente nel territorio - ad esempio, una persona che, dal territorio di un paese terzo, ottenga un accesso illecito (hacking) ad un sistema di informazioni che si trova nel territorio dello Stato membro.

Considerato che non tutte le tradizioni giuridiche degli Stati membri riconoscono una giurisdizione extraterritoriale per tutti i tipi di reati, il paragrafo 3 consente loro di non applicare le regole di giurisdizione di cui al paragrafo 1 rispetto alle situazioni coperte dal paragrafo 1, lettere b) e c).

Il paragrafo 4 richiede ad ogni Stato membro di adottare anche le misure necessarie per stabilire la propria giurisdizione sui reati di cui agli articoli da 3 a 5 nei casi in cui rifiuta di

consegnare o estradare una persona sospettata o condannata per tali reati ad un altro Stato membro o ad un paese terzo.

Il paragrafo 5 riguarda i casi di competenza giurisdizionale multipla, e mira a garantire la piena cooperazione tra gli Stati membri in modo da concentrare, se possibile, i procedimenti in un solo Stato membro. A questo fine, si ricorda che gli Stati membri possono fare ricorso a qualsiasi organismo o meccanismo istituito all'interno dell'Unione europea per agevolare la cooperazione tra le loro autorità giudiziarie e il coordinamento del loro operato. Tra questi anche Eurojust e la Rete giudiziaria europea.

Il paragrafo 6 dispone che gli Stati membri informano il Segretariato generale del Consiglio e la Commissione quando decidono di applicare il paragrafo 3.

Articolo 12 – Scambio di informazioni

Lo scopo dell'articolo 12 è quello di facilitare lo scambio di informazioni garantendo la presenza di punti di contatto operativi. Questo punto è importante per una cooperazione effettiva tra forze di polizia. In particolare, la necessità per tutti gli Stati membri di entrare a far parte della rete di punti di contatto del G8 è stata riconosciuta dal Consiglio Giustizia e affari interni il 19 marzo 1998 e più di recente quando ha adottato una raccomandazione del Consiglio sui punti di contatto accessibili 24 ore al giorno ai fini della lotta contro la criminalità ad alta tecnologia[36].

Articolo 13 - Attuazione

L'articolo 13 riguarda l'attuazione ed il seguito da dare alla presente decisione quadro. Gli Stati membri sono tenuti ad adottare le misure necessarie per conformarsi alla presente decisione quadro entro il 31 dicembre 2003.

Gli Stati membri trasmettono, entro tale data, al Segretariato generale del Consiglio e alla Commissione le disposizioni che danno attuazione nel loro diritto interno agli obblighi che gravano su di essi in virtù della presente decisione quadro. Il Consiglio valuta entro un anno, sulla base di tali informazioni e di una relazione scritta della Commissione, in che misura gli Stati membri abbiano adempiuto gli obblighi loro imposti dalla decisione quadro.

Articolo 14 – Entrata in vigore

L'articolo 14 dispone che la decisione quadro entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale delle Comunità europee*.

---

[36] GU C 187 del 3.7.2001, pag. 5.

2002/0086 (CNS)

Proposta di

DECISIONE-QUADRO DEL CONSIGLIO

relativa agli attacchi contro i sistemi di informazione

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sull'Unione europea, in particolare l'articolo 29, l'articolo 30, paragrafo 1, lettera a), l'articolo 31 e l'articolo 34, paragrafo 2, lettera b),

vista la proposta della Commissione[1],

visto il parere del Parlamento europeo[2],

considerando quanto segue:

(1) Si sono registrati attacchi contro sistemi di informazione, in particolare ad opera della criminalità organizzata, e aumentano le preoccupazioni per la possibilità di attacchi terroristici contro sistemi di informazione che fanno parte dell'infrastruttura critica degli Stati membri. Ciò costituisce una minaccia per la creazione di una società dell'informazione sicura e di uno spazio di libertà, sicurezza e giustizia, e richiede pertanto una risposta a livello di Unione europea.

(2) Una risposta efficace a queste minacce richiede un approccio globale rispetto alla sicurezza delle reti e dell'informazione, come evidenziato nel piano d'azione eEurope, nella comunicazione della Commissione "Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo"[3] e nella risoluzione del Consiglio del 6 dicembre 2001 relativa ad un approccio comune e ad azioni specifiche nel settore della sicurezza delle reti e dell'informazione.

(3) L'esigenza di accrescere ulteriormente la consapevolezza dei problemi relativi alla sicurezza dell'informazione e di fornire un'assistenza pratica è stata evidenziata anche nella risoluzione del Parlamento del 5 settembre 2001[4].

(4) Le rilevanti lacune e le notevoli differenze nelle normative degli Stati membri in questo settore ostacolano la lotta contro la criminalità organizzata ed il terrorismo e pregiudicano un'effettiva cooperazione giudiziaria e di polizia nel campo degli attacchi contro sistemi di informazione. Il carattere transnazionale e senza frontiere delle moderne reti di comunicazione elettronica fa sì che gli attacchi contro sistemi di informazione siano spesso di natura internazionale e rende evidente la necessità di

---

1 GU C..., pag.
2 GU C .., pag.
3 COM (2001) 298.
4 [2001/2098 (INI)]

adottare urgentemente azioni ulteriori per il ravvicinamento delle legislazioni penali in questo settore.

(5) Il piano d'azione del Consiglio e della Commissione sul modo migliore per attuare le disposizioni del trattato di Amsterdam concernenti uno spazio di libertà, sicurezza e giustizia[5], il Consiglio europeo di Tampere del 15-16 ottobre 1999, il Consiglio europeo di Santa Maria da Feira del 19-20 giugno 2000, la Commissione nel quadro di controllo[6] ed il Parlamento europeo nella sua risoluzione del 19 maggio 2000[7] contemplano o invocano iniziative legislative atte a contrastare la criminalità ad alta tecnologia, comprendenti definizioni, incriminazioni e sanzioni comuni.

(6) È necessario completare il lavoro svolto dalle organizzazioni internazionali, in particolare il lavoro di ravvicinamento delle legislazioni penali del Consiglio d'Europa ed il lavoro del G8 sulla cooperazione transnazionale in materia di criminalità ad alta tecnologia, mediante l'adozione di un approccio comune dell'Unione europea in questo settore. Questa esigenza è stata ulteriormente elaborata nella comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni "Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica"[8] .

(7) Le legislazioni penali nel settore degli attacchi a sistemi di informazione devono essere ravvicinate al fine di garantire la cooperazione giudiziaria e di polizia più ampia possibile nel settore dei reati attinenti ad attacchi a sistemi di informazione, e di contribuire alla lotta contro la criminalità organizzata ed il terrorismo.

(8) La decisione quadro sul mandato d'arresto europeo[9], l'allegato alla convenzione Europol e la decisione del Consiglio che ha istituito Eurojust contengono riferimenti alla criminalità informatica che devono essere definiti con maggiore precisione. Ai fini di tali strumenti, la criminalità informatica dev'essere intesa come comprensiva degli attacchi a sistemi di informazione quali definiti nella presente decisione quadro, che fornisce un livello molto più elevato di ravvicinamento degli elementi costitutivi di tali reati. La presente decisione quadro completa anche la decisione quadro sulla lotta al terrorismo[10] che si applica ad azioni terroristiche che cagionino danni sostanziali ad un'infrastruttura, quale anche un sistema di informazione, suscettibili di porre in pericolo la vita umana o di generare ingenti perdite economiche.

(9) Tutti gli Stati membri hanno ratificato la convenzione del Consiglio d'Europa del 28 gennaio 1981 sulla protezione delle persone rispetto al trattamento automatizzato di dati di carattere personale. I dati di carattere personale trattati nel quadro dell'attuazione della presente decisione quadro saranno protetti in conformità con i principi di detta convenzione.

---

5 GU C 19 del 23.1.1999.
6 COM (2001) 278 def.
7 A5-0127/2000
8 COM (2000) 890
9 GU C..., pag...
10 GU C..., pag...

(10) Per garantire un approccio coerente degli Stati membri nell'applicazione della presente decisione quadro, è importante avere, in questo settore, definizioni comuni, in particolare quelle di sistemi di informazione e di dati informatici.

(11) È necessario un approccio comune rispetto agli elementi costitutivi dei reati mediante la previsione di un reato comune di accesso illecito ad un sistema di informazione e di interferenza illecita con un sistema di informazione.

(12) È necessario evitare un'eccessiva criminalizzazione, specialmente per le condotte banali o di minore gravità, ed escludere la penalizzazione degli aventi diritto e delle persone autorizzate quali gli utenti legittimi, a titolo privato o professionale, i gestori, i controllori e gli operatori di reti e sistemi, i ricercatori scientifici e le persone autorizzate a collaudare un sistema, siano esse persone interne all'impresa o invece designate dall'esterno ed autorizzate a verificare la sicurezza di un sistema.

(13) È necessario che gli Stati membri prevedano, per gli attacchi ai danni di sistemi di informazione, pene effettive, proporzionate e dissuasive, tra cui anche, per i casi gravi, la custodia in carcere.

(14) È necessario prevedere pene più severe quando alcune circostanze che accompagnano un attacco contro un sistema di informazione ne fanno una minaccia ancora più seria per la società. In tali casi, le sanzioni comminate agli autori debbono essere tali da far rientrare gli attacchi contro sistemi di informazione nel campo di applicazione degli strumenti già adottati al fine di contrastare la criminalità organizzata, quali l'azione comune 98/733/GAI del 21 dicembre 1998, adottata dal Consiglio sulla base dell'articolo K.3 del trattato sull'Unione europea, relativa alla punibilità della partecipazione a un'organizzazione criminale negli Stati membri dell'Unione europea[11].

(15) È opportuno adottare misure volte a far sì che le persone giuridiche possano essere considerate responsabili per i reati di cui alla presente decisione quadro commessi a loro vantaggio e a garantire che ogni Stato membro stabilisca la sua giurisdizione sui reati commessi ai danni di sistemi di informazione nelle situazioni in cui l'autore è fisicamente presente sul suo territorio oppure il sistema di informazione è situato nel suo territorio.

(16) È altresì opportuno prevedere misure intese alla cooperazione tra Stati membri al fine di garantire un'azione efficace contro gli attacchi ai danni di sistemi di informazione, e in particolare istituire dei punti di contatto per lo scambio d'informazioni.

(17) Considerato che gli obiettivi di fare sì che gli attacchi contro sistemi di informazione siano puniti in tutti gli Stati membri con sanzioni penali effettive, proporzionate e dissuasive e di migliorare ed incoraggiare la cooperazione giudiziaria mediante la rimozione dei potenziali ostacoli non possono essere sufficientemente realizzati dagli Stati membri singolarmente, in quanto le norme devono essere comuni e compatibili, e possono pertanto essere realizzati meglio a livello di Unione, l'Unione è legittimata ad adottare misure, conformemente con il principio di sussidiarietà di cui all'articolo 2 del trattato UE e all'articolo 5 del trattato CE. In conformità con il

---

11 GU L 351 del 29.12.1998, pag. 1.

principio di proporzionalità, di cui all'articolo menzionato da ultimo, la presente decisione quadro non va al di là di quanto necessario per il raggiungimento dei suddetti obiettivi.

(18) La presente decisione quadro non pregiudica i poteri della Comunità europea.

(19) La presente decisione quadro rispetta i diritti fondamentali ed osserva i principi riconosciuti segnatamente nella Carta dei diritti fondamentali dell'Unione europea, in particolare i capi II e VI.

HA ADOTTATO LA PRESENTE DECISIONE QUADRO:

Articolo 1

Ambito d'applicazione e obiettivi

L'obiettivo della presente decisione quadro è quello di migliorare la cooperazione tra le autorità giudiziarie e tra le altre autorità competenti degli Stati membri, quali la polizia e gli altri servizi specializzati incaricati dell'applicazione della legge, mediante il ravvicinamento delle normative penali degli Stati membri nel settore degli attacchi contro sistemi di informazione.

Articolo 2

Definizioni

1. Ai fini della presente decisione quadro, si applicano le seguenti definizioni:

a) per *"reti di comunicazione elettronica"* s'intendono i sistemi di trasmissione e, se del caso, le apparecchiature di commutazione ("switching") o di instradamento ("routing") e altre risorse che consentono di trasportare segnali con mezzi a filo, radio, ottici o con altri mezzi elettromagnetici, comprese le reti satellitari, le reti terrestri fisse (a commutazione di circuito o di pacchetto, compreso Internet) e mobili, i sistemi elettrici a cavo, nella misura in cui siano usati per trasmettere segnali, le reti usate per l'emissione radiofonica e televisiva, e le reti di teledistribuzione via cavo, indipendentemente dal tipo di informazione trasportato.

b) per *"computer"* s'intende qualsiasi apparecchiatura o gruppo di apparecchi interconnessi o collegati, uno o più dei quali svolge un trattamento automatico di dati informatici secondo un programma

c) per *"dati informatici"* s'intende qualsiasi rappresentazione di fatti, informazioni o concetti creata o trasformata in modo tale da poter essere trattata da un sistema di informazione, compreso un programma atto far svolgere una funzione ad un sistema di informazione

d) per *"sistema di informazione"* s'intendono computer e reti elettroniche di comunicazione, nonché dati informatici immagazzinati, trattati, estratti o trasmessi dagli stessi ai fini della loro gestione, uso, protezione e manutenzione

e) per *“persona giuridica”* s'intende qualsiasi ente che abbia tale qualifica ai sensi della legislazione applicabile, eccetto gli Stati e altri organismi pubblici nell'esercizio dell'autorità statuale e le organizzazioni internazionali

f) per *"persona autorizzata"* s'intende qualsiasi persona fisica o giuridica che abbia il diritto, per contratto o per legge, oppure il permesso legittimo di usare, gestire, sorvegliare, collaudare, condurre ricerche scientifiche legittime o in altro modo operare un sistema di informazione e che agisce in conformità con tale dritto o permesso

g) l'espressione *"senza diritto"* significa che la condotta delle persone autorizzate o altre condotte riconosciute lecite dalla legislazione nazionale sono escluse.

Articolo 3

Accesso illecito a sistemi di informazione

Gli Stati membri provvedono a che l'accesso intenzionale, senza diritto, ad un sistema di informazione o ad una parte dello stesso sia punito come reato qualora sia commesso:

i) nei confronti di una qualsiasi parte di un sistema di informazione sottoposto a misure di protezione specifiche; o

ii) con l'intento di cagionare danni ad una persona fisica o giuridica; o

iii) con l'intento di procurare un vantaggio economico.

Articolo 4

Interferenza illecita con sistemi di informazione

Gli Stati membri provvedono a che le seguenti condotte intenzionali, senza diritto, siano punite come reato:

a) il fatto di ostacolare gravemente o interrompere il funzionamento di un sistema di informazione mediante l'immissione, la trasmissione, il danneggiamento, la cancellazione, il deterioramento, l'alterazione, la soppressione di dati informatici o rendendoli inaccessibili;

b) il fatto di cancellare, deteriorare, alterare, sopprimere o rendere inaccessibili dati informatici in un sistema di informazione qualora ciò venga commesso nell'intento di cagionare un danno a persone fisiche o giuridiche.

Articolo 5

Istigazione, favoreggiamento, complicità e tentativo

1. Gli Stati membri provvedono a che l'istigazione, il favoreggiamento, la complicità e il tentativo nella commissione dei reati di cui agli articoli 3 e 4 siano puniti come reato.

2. Gli Stati membri provvedono a che il tentativo di commettere i reati di cui agli articoli 3 e 4 sia punito come reato.

Articolo 6

Pene

1. Gli Stati membri provvedono a che i reati di cui agli articoli 3, 4 e 5 siano punibili con sanzioni effettive, proporzionate e dissuasive, tra cui anche la custodia in carcere per un periodo non inferiore, nel massimo, a un anno nei casi gravi. La nozione di casi gravi si deve intendere come volta ad escludere i casi in cui la condotta non abbia cagionato alcun danno né alcun profitto economico.

2. Gli Stati membri prevedono la possibilità di comminare sanzioni pecuniarie in aggiunta o in sostituzione delle pene detentive.

Articolo 7

Circostanze aggravanti

1. Gli Stati membri provvedono a che i reati di cui agli articoli 3, 4 e 5 siano punibili con pene detentive non inferiori, nel massimo, a quattro anni qualora siano stati commessi in presenza delle seguenti circostanze:

   a) il reato è stato commesso nell'ambito di un'organizzazione criminale come definita nell'azione comune 98/733/GAI del 21 dicembre 1998 relativa alla punibilità della partecipazione a un'organizzazione criminale negli Stati membri dell'Unione europea, a parte il livello di pena ivi previsto;

   b) il reato ha cagionato, o ha dato origine a, perdite economiche ingenti dirette o indirette, un danno corporale ad una persona fisica o un danno rilevante ad una parte dell'infrastruttura critica dello Stato membro;

   c) il reato ha procurato proventi elevati.

2. Gli Stati membri provvedono affinché i reati di cui agli articoli 3 e 4 siano punibili con pene detentive più severe di quelle previste all'articolo 6, qualora l'autore sia stato condannato con sentenza definitiva in uno Stato membro per un tale reato.

Articolo 8

Circostanze particolari

In deroga agli articoli 6 e 7, gli Stati membri prevedono che le pene di cui agli articoli 6 e 7 possano essere ridotte qualora, secondo l'autorità giudiziaria competente, l'autore abbia cagionato solo un danno di lieve entità.

Articolo 9

Responsabilità delle persone giuridiche

1. Gli Stati membri provvedono a che le persone giuridiche possano essere ritenute responsabili dei reati di cui agli articoli 3, 4 e 5 commessi a loro beneficio da qualsiasi soggetto, che agisca a titolo individuale o in quanto membro di un organo della persona giuridica, il quale detenga una posizione preminente in seno alla persona giuridica stessa, basata:

   a) sul potere di rappresentanza di detta persona giuridica

   b) sul potere di prendere decisioni per conto della persona giuridica

   c) sull'esercizio di poteri di controllo in seno a tale persona giuridica.

2. Oltre che nei casi di cui al paragrafo 1, gli Stati membri adottano le misure necessarie affinché le persone giuridiche possano essere ritenute responsabili qualora la mancata sorveglianza o il mancato controllo da parte di un soggetto tra quelli di cui al paragrafo 1 abbia reso possibile la commissione dei reati di cui agli articoli 3, 4 e 5 a beneficio della persona giuridica da parte di una persona soggetta alla sua autorità.

3. La responsabilità delle persone giuridiche ai sensi dei paragrafi 1 e 2 non esclude l'avvio di procedimenti penali contro le persone fisiche che abbiano commesso i reati o tenuto i comportamenti di cui agli articoli 3, 4 e 5.

Articolo 10

Sanzioni applicabili alle persone giuridiche

1. Gli Stati membri provvedono a che alla persona giuridica ritenuta responsabile ai sensi del paragrafo 1 dell'articolo 9 siano applicabili sanzioni efficaci, proporzionate e dissuasive, che comprendano sanzioni pecuniarie penali o non penali e che possano comprendere anche altre sanzioni quali:

   a) misure di esclusione dal godimento di un beneficio o aiuto pubblico,

   b) misure di divieto temporaneo o permanente di esercitare un'attività commerciale

   c) assoggettamento a sorveglianza giudiziaria o

   d) provvedimenti giudiziari di scioglimento.

2. Gli Stati membri provvedono a che alle persone giuridiche ritenute responsabili ai sensi del paragrafo 2 dell'articolo 9 siano applicate sanzioni o provvedimenti efficaci, proporzionati e dissuasivi.

Articolo 11

Giurisdizione

1. Ciascuno Stato membro adotta le misure necessarie a stabilire la propria giurisdizione sui reati di cui agli articoli 3, 4 e 5 laddove i reati siano stati commessi:

   a) interamente o in parte sul suo territorio o

b) da un suo cittadino, ai danni di individui o gruppi dello Stato stesso, o

c) a beneficio di una persona giuridica che ha la sua sede principale nel territorio dello Stato membro stesso.

2. Nello stabilire la propria giurisdizione ai sensi del paragrafo 1, lettera a), ogni Stato membro provvede a che tale giurisdizione abbracci i casi in cui:

a) l'autore abbia commesso il reato mentre era fisicamente presente nel suo territorio, indipendentemente dal fatto che il sistema di informazione contro il quale è stato commesso il reato si trovi o meno nel suo territorio, o

b) il sistema di informazione contro il quale è stato commesso il reato si trova nel suo territorio, indipendentemente dal fatto che l'autore del reato fosse o meno fisicamente presente nel suo territorio al momento della commissione del reato.

3. Uno Stato membro può decidere di non applicare o di applicare solo in situazioni o circostanze specifiche le regole di giurisdizione di cui al paragrafo 1, lettere b) e c).

4. Ciascuno Stato membro adotta le misure necessarie anche per stabilire la propria giurisdizione sui reati di cui agli articoli da 3 a 5 nei casi in cui rifiuta di consegnare o estradare una persona sospettata o condannata per tali reati ad un altro Stato membro o ad un paese terzo.

5. Qualora un reato rientri nella giurisdizione di più di uno Stato membro e quando ciascuno degli Stati interessati potrebbe validamente avviare un'azione penale sulla base degli stessi fatti, gli Stati membri interessati cooperano per decidere quale di essi perseguirà gli autori del reato allo scopo, se possibile, di concentrare i procedimenti in un solo Stato membro. A tal fine, gli Stati membri possono fare ricorso a qualsiasi organismo o meccanismo istituito all'interno dell'Unione europea per agevolare la cooperazione tra le loro autorità giudiziarie ed il coordinamento del loro operato.

6. Qualora decidano di avvalersi del paragrafo 3, gli Stati membri ne informano il Segretariato generale del Consiglio e la Commissione, precisando, ove necessario, i casi e le circostanze specifiche in cui si applica tale decisione

Articolo 12

Scambio di informazioni

1. Gli Stati membri stabiliscono dei punti di contatto operativi, disponibili ventiquattr'ore su ventiquattro e sette giorni su sette, per lo scambio delle informazioni relative ai reati di cui agli articoli 3, 4 e 5, fatte salve le disposizioni sulla protezione dei dati personali.

2. Ciascuno Stato membro informa il Segretariato generale del Consiglio e la Commissione in merito al proprio punto di contatto operativo stabilito per lo scambio d'informazioni riguardo ai reati che comportano attacchi a sistemi di informazione. Il Segretariato generale trasmette tali informazioni agli altri Stati membri.

Articolo 13

Attuazione

1. Gli Stati membri adottano le disposizioni necessarie per conformarsi alla presente decisione quadro entro il 31 dicembre 2003.

2. Gli Stati membri comunicano al Segretariato generale del Consiglio ed alla Commissione il testo delle disposizioni da essi adottate e le informazioni su ogni altra misura presa per conformarsi alla presente decisione quadro.

3. Su questa base, la Commissione presenta, entro il 31 dicembre 2004, una relazione al Parlamento europeo ed al Consiglio sull'applicazione della presente decisione quadro, accompagnata, se necessario, da proposte legislative.

4. Il Consiglio valuta in che misura gli Stati membri si siano conformati alla presente decisione quadro.

Articolo 14

Entrata in vigore

La presente decisione quadro entra in vigore il ventesimo giorno successivo alla sua pubblicazione nella *Gazzetta ufficiale delle Comunità europee*.

Fatto a Bruxelles,

Per il Consiglio
Il Presidente