



COMMISSIONE DELLE COMUNITÀ EUROPEE

Bruxelles, 26.1.2001  
COM(2000) 890 definitivo

**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**

**eEurope  
2002**

## Sommario

La transizione dell'Europa verso la società dell'informazione è contraddistinta da profondi mutamenti in tutti gli ambiti della vita umana: lavoro, istruzione e tempo libero, governo, industria e commercio. Le nuove tecnologie dell'informazione e delle comunicazioni stanno rivoluzionando le nostre economie e società. Il successo della società dell'informazione è importante per la crescita, la concorrenzialità e le possibilità occupazionali in Europa e ha profonde implicazioni sotto il profilo economico, sociale e giuridico.

A dicembre del 1999 la Commissione ha lanciato l'iniziativa 'eEurope' (Europa telematica) con l'intento di garantire che l'Europa fruisca dei vantaggi offerti dalle tecnologie digitali e affinché la società dell'informazione che si sta delineando coinvolga l'intera società. A giugno del 2000, il Consiglio europeo di Feira ha approvato un piano d'azione globale per l'Europa telematica ('eEurope Action Plan'), sollecitandone l'attuazione entro la fine dell'anno 2002. Il piano d'azione enfatizza l'importanza della sicurezza delle reti e della lotta alla criminalità telematica.

Le infrastrutture dell'informazione e delle comunicazioni sono diventate un elemento critico delle nostre economie. Sfortunatamente, dette infrastrutture presentano dei punti vulnerabili e offrono nuove possibilità di comportamenti criminali, che possono assumere una grande varietà di forme e avere una portata transnazionale. Sebbene, per diversi motivi, manchino dati statistici attendibili, non vi è dubbio che i reati informatici costituiscono una minaccia per gli investimenti e le attività degli operatori del settore, nonché per la sicurezza e la fiducia nella società dell'informazione. Si dice che alcuni recenti episodi d'interruzione di servizio e di attacchi mediante virus informatici abbiano causato ingenti danni finanziari.

È possibile agire per prevenire le attività criminali sia aumentando la sicurezza delle infrastrutture dell'informazione sia facendo in modo che le autorità preposte all'applicazione della legge dispongano di opportuni strumenti d'intervento, nel pieno rispetto dei diritti fondamentali dei cittadini.

L'Unione europea ha già adottato alcune misure per combattere la diffusione su Internet di informazioni con contenuto nocivo e illegale, per tutelare la proprietà intellettuale e i dati personali, per promuovere il commercio elettronico e l'uso di firme elettroniche, nonché per accrescere la sicurezza delle operazioni telematiche. Ad aprile del 1998, la Commissione ha presentato al Consiglio i risultati di uno studio sulla criminalità informatica (noto come 'studio COMCRIME'). A ottobre del 1999, nelle conclusioni del vertice svoltosi a Tampere, il Consiglio europeo ha affermato che ci si dovrebbe sforzare di concordare definizioni e sanzioni comuni anche per la criminalità ad alta tecnologia. Il Parlamento europeo ha inoltre auspicato l'adozione di definizioni collettivamente concordate dei reati informatici e l'armonizzazione della normativa, in particolare del diritto penale (sostanziale). Il Consiglio dell'Unione europea ha adottato una posizione comune in merito ai negoziati condotti in seno al Consiglio d'Europa sulla criminalità telematica ed ha adottato alcuni elementi iniziali di una strategia comunitaria contro la criminalità ad alta tecnologia. Alcuni Stati membri hanno inoltre svolto un ruolo di primo piano nel quadro delle attività condotte in materia in seno al G8.

La presente comunicazione analizza la necessità e le eventuali forme di un'iniziativa politica globale per migliorare la sicurezza delle infrastrutture dell'informazione e per combattere la criminalità telematica, nel contesto degli obiettivi di più ampio respiro della *Società dell'informazione* e del progetto '*Libertà, sicurezza e giustizia*', conformemente all'impegno dell'Unione europea di rispettare i diritti fondamentali dell'uomo.

A breve termine, la Commissione ritiene che sia palese l'esigenza di uno strumento comunitario che garantisca che gli Stati membri contemplino sanzioni efficaci contro la pornografia infantile su Internet. La Commissione presenterà quest'anno una proposta di decisione quadro che contempli, nel contesto più ampio di un pacchetto riguardante le problematiche connesse allo sfruttamento sessuale dei minori e alla tratta degli esseri umani, delle misure per l'avvicinamento delle normative e delle sanzioni.

A lungo termine, la Commissione intende presentare proposte legislative per un ulteriore ravvicinamento del diritto penale sostanziale e del diritto processuale penale in materia di criminalità ad alta tecnologia. Conformemente alle conclusioni del Consiglio europeo di Tampere di ottobre del 1999, la Commissione esaminerà inoltre le varie alternative per il mutuo riconoscimento dei provvedimenti istruttori connessi a reati informatici.

Parallelamente, la Commissione intende promuovere l'istituzione a livello nazionale, laddove non siano ancora state istituite, di unità di polizia specializzate in criminalità informatica, appoggiare l'adeguata formazione tecnica del personale addetto all'applicazione della legge nonché favorire le iniziative europee per la sicurezza dell'informazione.

Sul piano tecnico ed in conformità al quadro giuridico, la Commissione intende promuovere la ricerca e lo sviluppo (R&S) volti a comprendere e limitare i punti vulnerabili, a favorire l'applicazione della legge e ad incentivare la divulgazione delle conoscenze specifiche.

La Commissione intende inoltre istituire un Forum europeo cui aderiscano gli organismi preposti all'applicazione della legge, i prestatori di servizi Internet, i gestori di telecomunicazioni, le organizzazioni per la tutela dei diritti civili, i rappresentanti di consumatori ed i garanti della protezione dei dati, nonché altre parti interessate, allo scopo di migliorare la reciproca comprensione e la cooperazione a livello comunitario. Il Forum si adopererà per: sensibilizzare il pubblico mettendolo in guardia dalla minaccia rappresentata dai criminali telematici operanti sull'Internet; promuovere la pratica per la sicurezza; individuare efficaci strumenti e procedure contro la criminalità informatica; incoraggiare l'ulteriore sviluppo di meccanismi di allertamento precoce e di gestione di crisi.

## **INVITO A PRESENTARE OSSERVAZIONI CIRCA LA PRESENTE COMUNICAZIONE**

**La Commissione europea sollecita tutte le parti interessate a trasmettere osservazioni circa le problematiche trattate dalla presente comunicazione. Le eventuali osservazioni possono essere inviate entro il 23.3. 2001 al seguente indirizzo di posta elettronica:**

**Info-jai-cybercrime-comments@cec.eu.int**

**In linea di massima, le osservazioni saranno pubblicate su Internet, salvo espressa richiesta in senso contrario da parte dell'autore. I contributi anonimi non saranno pubblicati. La Commissione si riserva il diritto di non pubblicare le osservazioni pervenute (ad esempio qualora formulate mediante linguaggio offensivo). Le osservazioni potranno essere consultate mediante un collegamento ipertestuale al seguente sito Internet:**

**<http://Europa.eu.int/ISPO/eif/InternetPolicies/Crime/crime1.html>**

**Al suddetto indirizzo sono inoltre disponibili eventuali suggerimenti circa il formato tecnico ed informazioni circa la politica relativa alle pubblicazioni. Si consiglia di visitare il sito prima d'inviare le eventuali osservazioni.**

### **AUDIZIONE PUBBLICA**

**La Commissione europea intende inoltre organizzare un'audizione pubblica sulle problematiche trattate dalla presente comunicazione, cui potranno partecipare le parti interessate. Tale audizione si svolgerà il 7.3. 2001. Le domande d'invito a presentare una dichiarazione durante tale audizione devono essere inviate per via elettronica entro il 20.2. 2001 al seguente indirizzo di posta elettronica:**

**Info-jai-cybercrime-hearing@cec.eu.int**

**o per lettera al seguente indirizzo:**

**Commissione europea  
Ufficio BU33-5/9  
200 Wetstraat/Rue de la Loi  
B-1049 Bruxelles  
Belgio**

**La Commissione europea si riserva il diritto di selezionare le parti che intervengono. Tale selezione sarà fatta in funzione del numero di richieste e con l'intento di garantire l'audizione di un ampio spettro di interessi.**

# INDICE

## Sommario

- 1. LA SOCIETÀ DELL'INFORMAZIONE: OPPORTUNITÀ E RISCHI**
  - 1.1. Strategie a livello nazionale ed internazionale**
- 2. SICUREZZA DELLE INFRASTRUTTURE DELL'INFORMAZIONE**
- 3. REATI CONNESSI AI SISTEMI INFORMATICI**
- 4. QUESTIONI DI DIRITTO SOSTANZIALE**
- 5. QUESTIONI DI DIRITTO PROCESSUALE**
  - 5.1. Intercettazione di comunicazioni**
  - 5.2. Conservazione di dati relativi alle comunicazioni**
  - 5.3. Accesso ed utilizzo anonimo**
  - 5.4. Cooperazione concreta a livello internazionale**
  - 5.5. Poteri e giurisdizione in materia di procedura penale**
  - 5.6. Valore probatorio dei dati informatici**
- 6. MISURE NON LEGISLATIVE**
  - 6.1. Unità speciali a livello nazionale**
  - 6.2. Formazione specializzata**
  - 6.3. Migliori informazioni e norme comuni per la registrazione dei dati**
  - 6.4. Cooperazione tra i vari soggetti: Forum UE**
  - 6.5. Azioni dirette degli operatori del settore**
  - 6.6. Progetti di RST finanziati dall'UE**
- 7. CONCLUSIONI E PROPOSTE**
  - 7.1. Proposte legislative**
  - 7.2. Proposte di carattere non legislativo**
  - 7.3. Iniziative in altre sedi internazionali**

## 1. LA SOCIETÀ DELL'INFORMAZIONE: OPPORTUNITÀ E RISCHI

La crescente accessibilità ed il sempre più diffuso impiego delle tecnologie della società dell'informazione (TSI) e la mondializzazione dell'economia sono caratteristiche della nostra epoca. L'ulteriore sviluppo tecnologico e la diffusione dell'uso di reti aperte, quali Internet, negli anni a venire sarà fonte di nuove grandi possibilità e nuove sfide.

Nella riunione al vertice di Lisbona a marzo del 2000, il Consiglio europeo 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 'eEurope' per trarre il massimo vantaggio da questa opportunità.<sup>1</sup> Il suddetto piano d'azione - preparato dalla Commissione e dal Consiglio, e approvato in occasione della riunione al vertice del Consiglio europeo a Feira nel giugno 2000 - prevede l'adozione entro la fine dell'anno 2002 di azioni volte a promuovere la sicurezza delle reti e l'adozione di una strategia coordinata e coerente per far fronte alla criminalità informatica.<sup>2</sup>

L'infrastruttura dell'informazione è diventata un elemento critico della struttura portante delle nostre economie. Gli utilizzatori dovrebbero poter contare sulla disponibilità dei servizi d'informazione ed avere la certezza che non si possa accedere o modificare abusivamente le loro comunicazioni e dati. Questa è la premessa per il decollo del commercio elettronico e la piena realizzazione della società dell'informazione.

Le nuove tecnologie digitali e senza filo sono già diventate onnipresenti. Grazie ad esse si è liberi di spostarsi pur restando collegati, ossia conservando il contatto con una miriade di servizi basati su una struttura complessa di reti. Grazie ad esse è possibile partecipare, insegnare e apprendere, giocare e lavorare assieme ad altri, essere coinvolti nel processo politico. Tuttavia, col crescere della dipendenza delle società da queste tecnologie occorrono degli efficaci strumenti tecnici e giuridici per riuscire a gestire i rischi connessi al loro uso.

Le tecnologie della società dell'informazione (TSI) possono essere usate, e vengono di fatto utilizzate, per condurre ed favorire diverse attività criminose. Nelle mani di individui operanti in mala fede, con intento doloso o con grave negligenza, queste tecnologie possono diventare degli strumenti per attività che mettono in pericolo o compromettono la vita, il patrimonio o la dignità delle persone o ledono l'interesse della collettività.

La strategia classica in materia di sicurezza richiede una rigorosa compartimentazione organizzativa, geografica e strutturale dell'informazione in funzione della sua sensibilità e classificazione. Questa prassi non è più realmente attuabile nel mondo digitale a causa della distribuzione del trattamento delle informazioni, della possibilità dei servizi di seguire gli utenti mobili e del requisito dell'interoperabilità. Le tradizionali procedure di sicurezza stanno per essere soppiantate da soluzioni innovative supportate da tecnologie emergenti. Queste si basano sul ricorso alla crittazione e alle firme elettroniche, a nuovi strumenti per il controllo dell'accesso e l'autenticazione, nonché filtri di software di ogni genere<sup>3</sup>. Le tecnologie da sole

---

<sup>1</sup> 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>.

<sup>2</sup> [http://europa.eu.int/comm/information\\_society/eeurope/actionplan/index\\_en.htm](http://europa.eu.int/comm/information_society/eeurope/actionplan/index_en.htm).

<sup>3</sup> I flussi d'informazione sono filtrati e controllati a tutti i livelli: dal programma 'firewall' che esamina tutti i pacchetti di dati, attraverso il filtro che individua i programmi concepiti con finalità di dolo, poi attraverso il filtro della posta elettronica che elimina con discrezione i messaggi indesiderati (spamming), fino al filtro browser che impedisce l'accesso a materiale dannoso.

non bastano a garantire delle infrastrutture d'informazione sicure e affidabili, occorre anche che queste siano strutturate in modo corretto ed utilizzate in modo efficiente. Alcune di queste tecnologie sono già disponibili, ma spesso gli utilizzatori ne ignorano l'esistenza, non sanno come servirsene o non sanno in che casi possono essere addirittura indispensabili.

### 1.1. Strategie a livello nazionale e internazionale

I reati informatici sono commessi nel cibernazio ed hanno una portata transnazionale, superano cioè i confini di stato convenzionali. In linea di principio, possono essere commessi da qualsiasi luogo e a danno di qualsiasi utilizzatore di computer nel mondo. La necessità di combattere la criminalità informatica sia a livello nazionale che internazionale è universalmente riconosciuta<sup>4</sup>.

A livello nazionale, spesso mancano ancora meccanismi globali e inquadrati in un'ottica internazionale per far fronte alle nuove sfide della sicurezza della rete e della criminalità informatica. Nella maggioranza dei paesi, i meccanismi per contrastare i reati informatici sono focalizzati sul diritto nazionale (particolarmente quello penale) e trascurano provvedimenti di prevenzione alternativi.

Nonostante gli sforzi delle organizzazioni internazionali e sovranazionali, le varie normative nazionali vigenti nel mondo presentano notevoli divergenze, soprattutto per quanto riguarda le disposizioni penali in materia di accesso abusivo a sistemi o reti informatiche, di tutela dei segreti commerciali e di contenuti illeciti. Notevoli differenze esistono inoltre per quanto riguarda i poteri di coercizione degli organismi incaricati delle indagini (soprattutto in relazione ai dati crittati e alle indagini su reti internazionali), la delimitazione della giurisdizione in questioni penali, nonché per quanto riguarda la responsabilità dei prestatori di servizi intermediari, da un lato, e dei fornitori di contenuti dall'altro. La direttiva 2000/31/CE<sup>5</sup> sul commercio elettronico modifica questa situazione per quanto riguarda la responsabilità dei prestatori di servizi intermediari per talune loro attività. La direttiva vieta inoltre agli Stati membri di imporre a tali prestatori intermediari di servizi l'obbligo generale di controllare le informazioni da essi trasmesse o memorizzate.

Sul piano internazionale e sovranazionale, è stata ampiamente riconosciuta la necessità di combattere efficacemente la criminalità informatica e diverse organizzazioni coordinano o cercano di armonizzare le attività in questo campo. Nel dicembre del 1997, i ministri della giustizia e degli interni riuniti nell'ambito del G8 hanno adottato un catalogo di principi ed un piano d'azione articolato in 10 punti, sottoscritto dai rappresentanti riuniti nell'incontro al vertice di Birmingham di maggio 1998 e attualmente in fase d'applicazione.<sup>6</sup> A febbraio del 1997 il Consiglio d'Europa (in appresso 'C.d.E.') ha iniziato a redigere una convenzione

---

<sup>4</sup> Cfr. ad es. il Piano d'azione *e-Europe* al sito: [http://Europa.eu.int/comm/information\\_society/eeurope/ACHCNtionplan/index\\_en.htm](http://Europa.eu.int/comm/information_society/eeurope/ACHCNtionplan/index_en.htm) e le dichiarazioni del sig. Antonio Vitorino al sito: [http://Europa.eu.int/comm/commissioners/vitorino/speeches/2000/septembre/2000-1909-en\\_brussels.pdf](http://Europa.eu.int/comm/commissioners/vitorino/speeches/2000/septembre/2000-1909-en_brussels.pdf) nonché le dichiarazioni del Primo ministro francese Lionel Jospin al sito: <http://www.france.diplomatie.fr/actual/evenements/cybercrim/jospin.gb.html>.

<sup>5</sup> Direttiva 2000/31/CE del Parlamento europeo e del Consiglio dell'8 giugno 2000 relativa a taluni aspetti giuridici dei servizi della società dell'informazione, in particolare il commercio elettronico, nel mercato interno («Direttiva sul commercio elettronico»).

<sup>6</sup> Il Consiglio dei ministri GAI dell'Unione europea del 19 marzo 1998 ha approvato i 10 principi della lotta contro la criminalità ad alta tecnologia, adottati dal G8 ed ha esortato gli Stati membri dell'UE non partecipanti al G8 di predisporre ad aderire alla suddetta rete. Reperibile al sito della Rete giudiziaria europea: <http://ue.eu.int/ejn/index.htm>.

internazionale sulla criminalità telematica ('cibercriminalità') i cui lavori si prevede saranno completati nel 2001.<sup>7</sup> La lotta alla criminalità telematica è inclusa nel programma delle discussioni bilaterali della Commissione con taluni governi (non appartenenti all'UE) È stata istituita una task force comune CE/USA per la protezione dell'infrastruttura critica<sup>8</sup>.

L'ONU e l'OCSE si sono anch'esse cimentate in questo campo, che è trattato nell'ambito di consessi internazionali, quali il Global Business Dialogue e il Trans-Atlantic Business Dialogue<sup>9</sup>.

A livello dell'Unione europea, fino a qualche tempo fa, le azioni legislative si sono concretate essenzialmente in misure nel campo dei diritti d'autore, della tutela del diritto fondamentale alla riservatezza e alla protezione dei dati personali, dei servizi d'accesso condizionato, del commercio elettronico, delle firme elettroniche e soprattutto della liberalizzazione dei prodotti per la crittazione, misure che sono indirettamente connesse alla criminalità informatica.

Negli ultimi tre o quattro anni è stata inoltre adottata una serie d'importanti misure di carattere non legislativo. Tra queste vi è il piano d'azione contro le informazioni di contenuto illegale e nocivo diffuse su Internet, che concorre a finanziare azioni di sensibilizzazione, esperimenti di valutazione e filtraggio dei contenuti, l'istituzione di 'hot-lines' ed iniziative per la tutela dei minori e della dignità umana nella società dell'informazione, la lotta alla pornografia infantile e le intercettazioni di comunicazioni nell'ambito di operazioni per l'applicazione della legge.<sup>10</sup> L'Unione europea, che da molto tempo finanzia progetti di R&S volti a promuovere la sicurezza e la fiducia nelle infrastrutture informatiche e nelle operazioni elettroniche, ha recentemente incrementato gli stanziamenti di bilancio relativi al programma TSI. I progetti di ricerca ed operativi, volti a promuovere l'addestramento specializzato degli addetti all'applicazione della legge e la cooperazione tra autorità preposte all'applicazione della legge

---

<sup>7</sup> Il testo provvisorio è disponibile in due lingue e reperibile su Internet all'indirizzo <http://conventions.coe.int/treaty/fr/projets/cybercrime.htm> (testo francese) e <http://conventions.coe.int/treaty/en/projets/cybercrime.htm> (testo inglese).

<sup>8</sup> Sotto l'egida del gruppo consultivo paritetico istituito nel quadro dell'Accordo di cooperazione scientifica e tecnologica tra la Comunità europea e gli Stati Uniti d'America.

<sup>9</sup> Le Nazioni Unite hanno pubblicato un manuale completo intitolato "Manual on the prevention and control of computer-related crime," recentemente aggiornato. Nel 1983, l'OCSE ha condotto uno studio sulla possibilità di applicare e di armonizzare a livello internazionale le leggi del diritto penale per combattere il problema dei reati o degli abusi informatici. Nel 1986, ha pubblicato la relazione "Computer-Related Crime: Analysis of Legal Policy", in cui si analizzano le leggi esistenti e le proposte di riforma elaborate da alcuni Stati membri, e in cui si raccomanda un elenco minimo degli abusi per i quali gli Stati dovrebbero porre un divieto e che dovrebbero essere puniti ai sensi del diritto penale. Da ultimo, nel 1992, l'OCSE ha elaborato una serie di orientamenti per la sicurezza dei sistemi d'informazione, che dovrebbero costituire la base su cui gli Stati e gli operatori del settore privato potrebbero istituire un quadro per la sicurezza dei sistemi informatici.

<sup>10</sup> Raccomandazione del Consiglio 98/560/CE del 24 settembre 1998 concernente lo sviluppo della competitività dell'industria dei servizi audiovisivi e d'informazione europei attraverso la promozione di strutture nazionali volte a raggiungere un livello comparabile e efficace di tutela dei minori e della dignità umana; Libro verde sulla tutela dei minori e della dignità umana nei servizi audiovisivi e di informazione; COM(96) 483, ottobre 1996, <http://europa.eu.int/en/record/green/gp9610/protec.htm>; Comunicazione della Commissione al Consiglio, al Parlamento europeo, al Comitato economico e sociale e al Comitato delle regioni - Informazioni di contenuto illegale e nocivo su Internet (COM(96) 487 def.); Risoluzione sulla comunicazione della Commissione sulle informazioni di contenuto illegale e nocivo su Internet (COM(96) 487 - C4-0592/96); Risoluzione del Consiglio del 17 gennaio 1995 sull'intercettazione legale delle telecomunicazioni (GU C 329, del 4.11.1996, pp. 1-6).

ed operatori economici, sono inoltre finanziati nel quadro dei programmi relativi al terzo pilastro, quali i programmi STOP, FALCONE, OISIN e GROTIUS.<sup>11</sup>

Nell'ambito del piano d'azione per combattere la criminalità organizzata, approvato dal Consiglio GAI a maggio del 1997 e sottoscritto dal Consiglio europeo di Amsterdam, si richiedeva tra l'altro che la Commissione realizzasse uno studio sulla criminalità informatica entro la fine del 1998. Tale studio, denominato 'studio COMCRIME' è stato presentato dalla Commissione al gruppo di lavoro multidisciplinare per la lotta contro la criminalità organizzata istituito in seno al Consiglio nell'aprile del 1998<sup>12</sup>. La presente comunicazione costituisce il successivo elemento della risposta alla richiesta del Consiglio GAI.

Prima di redigere la presente comunicazione, la Commissione ha giudicato opportuno interpellare informalmente i rappresentanti delle autorità preposte all'applicazione della legge e delle autorità di controllo degli Stati membri competenti in materia di protezione dei dati<sup>13</sup>, nonché i rappresentanti degli operatori europei del settore (principalmente ISP e gestori di telecomunicazioni).<sup>14</sup>

La presente comunicazione esamina le varie possibilità di ulteriori azioni da parte dell'Unione europea contro la criminalità informatica, alla luce dell'analisi e delle raccomandazioni contenute nel suddetto studio, delle conclusioni tratte dal processo di consultazione, delle nuove possibilità offerte dal trattato di Amsterdam nonché dell'attività già svolta nell'ambito dell'UE, del G8 e del C.d.E. Le soluzioni scelte a livello dell'Unione europea non dovrebbero ostacolare il funzionamento del mercato interno o causarne la frammentazione, né dovrebbero comportare delle misure che pregiudichino la tutela dei diritti fondamentali<sup>15</sup>.

## **2. SICUREZZA DELLE INFRASTRUTTURE DELL'INFORMAZIONE**

Nella società dell'informazione, la vecchia generazione di reti di comunicazioni nazionali viene gradualmente soppiantata da reti mondiali controllate dagli utilizzatori. Una delle ragioni del successo di Internet è l'aver offerto agli utenti l'accesso alle tecnologie più

---

<sup>11</sup> [http://europa.eu.int/comm/justice\\_home/jai/prog\\_en.htm](http://europa.eu.int/comm/justice_home/jai/prog_en.htm).

<sup>12</sup> "Aspetti giuridici della criminalità informatica nella società dell'informazione – COMCRIME." Lo studio è stato elaborato dal Prof. U. Sieber dell'università di Würzburg nell'ambito di un contratto stipulato con la Commissione europea. La relazione finale può essere consultata all'indirizzo: <http://www2.echo.lu/legal/en/crime/crime.html>.

<sup>13</sup> A livello comunitario, le autorità di controllo competenti in materia di protezione dei dati personali costituiscono uno specifico gruppo istituito a norma dell'articolo 29 della direttiva 95/46/CE, che è l'organo consultivo indipendente dell'Unione europea, competente in materia di riservatezza e di protezione dei dati; cfr. gli artt. 29 e 30 della suddetta direttiva.

<sup>14</sup> Due riunioni con rappresentanti delle autorità giudiziarie si sono svolte il 10.12.99 e l'1.3.2000. Un incontro con gli operatori nel settore Internet si è tenuto il 13.3.2000. Un incontro con un numero ristretto di esperti nel campo della protezione dei dati personali è avvenuto il 31.3.2000. Un incontro finale con la partecipazione di tutti i suddetti rappresentanti si è svolto il 17.4.2000. I verbali delle suddette riunioni possono essere ottenuti inviando una richiesta scritta a uno dei seguenti indirizzi: Commissione europea, Unità INFSO/A5, Wetstraat/Rue de la Loi 200, 1049 Bruxelles, Belgio oppure Commissione europea, Unità JAI/B2, Wetstraat/Rue de la Loi 200, 1049 Bruxelles, Belgio.

<sup>15</sup> Cfr. La Carta dei diritti fondamentali dell'UE ([http://Europa.eu.int/comm/justice\\_home/unit/charte\\_fr.htm](http://Europa.eu.int/comm/justice_home/unit/charte_fr.htm)) e l'articolo 6 del Trattato sull'Unione europea, nonché la giurisprudenza della Corte di giustizia europea.

moderne. Secondo la legge di Moore<sup>16</sup> la potenza degli elaboratori raddoppia ogni 18 mesi. La tecnologia delle comunicazioni sta evolvendo ad un ritmo ancora più vorticoso<sup>17</sup>. Ciò porta al raddoppio del volume dei dati trasportati su Internet ad intervalli inferiori all'anno.

In passato le reti telefoniche classiche sono state costruite e gestite da organizzazioni nazionali. Gli utenti avevano una scelta limitata di servizi e non esercitavano alcun controllo sull'ambiente. Le prime reti di trasmissione dati sono state sviluppate secondo la stessa filosofia del controllo centrale dell'ambiente. La sicurezza all'interno di questi ambienti rifletteva questa concezione.

Internet e le altre nuove reti sono molto diverse e la sicurezza deve essere trattata in modo diverso. In tali reti le informazioni ed il controllo sono per lo più ubicati alla periferia, in corrispondenza degli utilizzatori e dei servizi. Il nucleo della rete è semplice ed efficiente, adibito essenzialmente alla trasmissione di dati. La verifica o il controllo del contenuto sono limitati. È solo alla destinazione finale che i bits si trasformano nel suono di una voce, nell'immagine di una radiografia o nella conferma di un'operazione bancaria. La responsabilità della sicurezza incombe pertanto in gran parte agli utenti, poiché solo essi possono stabilire il valore dei bits inviati o ricevuti e determinare il livello di protezione necessario.

L'ambiente utente costituisce pertanto un elemento chiave dell'infrastruttura dell'informazione. Le tecniche di sicurezza devono essere applicate in tal sede, con l'autorizzazione e la collaborazione dell'utente ed in funzione delle sue esigenze. Questo è particolarmente importante se si considera la crescente gamma di attività che si effettua da un'unica apparecchiatura terminale. La stessa apparecchiatura è utilizzata per lavorare e per svagarsi, per guardare la televisione e autorizzare bonifici bancari.

Molte sono le tecnologie di sicurezza disponibili ed altre ancora sono in fase di sviluppo. I vantaggi in termini di sicurezza dello sviluppo 'open source' diventano sempre più evidenti. Molto è stato fatto in materia di metodi formali e criteri di valutazione della sicurezza. L'uso delle tecnologie di crittazione e le firme digitali stanno diventando indispensabili, soprattutto con la diffusione dell'accesso senza fili. Occorre una sempre crescente varietà di meccanismi di autenticazione per soddisfare le diverse esigenze negli ambienti in cui si interagisce. In alcuni ambienti è necessario o si desidera restare anonimi, in altri è richiesta la prova del possesso di una determinata caratteristica, senza rivelare la propria identità, ad esempio nel caso si debba dimostrare di essere un utente adulto o un dipendente o un cliente di una determinata società. In altre situazioni ancora, è necessario dimostrare o rivelare la propria identità. Anche i filtri di software diventano sempre più sofisticati e permettono all'utente di proteggere se stesso, o chi è sotto la sua tutela, da informazioni che non volute, quali contenuti indesiderati, messaggi elettronici indesiderati ('spamming'), software pericoloso e altri tipi di attacchi. L'applicazione e la gestione di detti meccanismi di sicurezza necessari all'interno dell'Internet e delle nuove reti comporta inoltre notevoli costi per gli operatori del settore e gli utilizzatori. È pertanto importante incoraggiare l'innovazione e l'uso commerciale delle tecnologie e dei servizi per la sicurezza.

---

<sup>16</sup> Constatazione fatta nel 1965 da Gordon Moore, cofondatore di Intel, circa la velocità con cui aumenta la densità dei transistor integrati. Tale densità attualmente raddoppia circa ogni 18 mesi, e questo incide direttamente sul prezzo e la prestazione dei chip di elaboratore. Molti esperti prevedono che questo ritmo verrà mantenuto per almeno un altro decennio.

<sup>17</sup> La tecnologia più recente permette di trasportare contemporaneamente attraverso un solo cavo a fibre ottiche l'equivalente di 100 milioni di chiamate vocali.

Naturalmente, anche l'infrastruttura condivisa dei collegamenti di comunicazione e i 'name server' (i programmi che traducono gli indirizzi numerici in indirizzi alfabetici) presentano dei propri aspetti di sicurezza. La trasmissione dei dati dipende dai collegamenti fisici occorrenti per il loro instradamento da un elaboratore ad un altro. Questi collegamenti devono essere predisposti e protetti in modo da consentire la trasmissione anche in caso d'incidenti, attacchi o crescenti volumi di traffico. La comunicazione dipende inoltre da servizi critici, quali quelli forniti dai 'name server' sopra citati, ed in particolare dal 'root name server' (che gestisce il traffico di dati), che forniscono gli indirizzi richiesti. Ciascuno di questi elementi dev'essere anch'esso adeguatamente protetto, ed il livello di protezione può variare in funzione dello spazio per il nome ('name space') e della base di utilizzatori ('user base') servita.

Nell'intento d'incrementare la flessibilità e di far fronte alle esigenze degli utilizzatori, le tecnologie delle infrastrutture dell'informazione sono diventate sempre più complesse, spesso con un'inadeguata attenzione sul piano progettuale alla sicurezza. A ciò si aggiunga che la struttura complessa comporta un ricorso a programmi sempre più sofisticati e interconnessi, che talvolta presentano debolezze e lacune di sicurezza, che la rende facilmente esposta ad attacchi. Assumendo caratteristiche sempre più complesse e servendosi di elementi sempre più sofisticati, il ciberspazio rivela nuovi ed imprevisi punti vulnerabili.

Esistono già diversi dispositivi tecnologici, ed altri se ne stanno sviluppando, per migliorare la sicurezza nel ciberspazio. La strategia comprende misure volte a:

- rendere sicuri / proteggere gli elementi critici dell'infrastruttura, mediante l'impiego di infrastrutture a chiave privata (PKI), lo sviluppo di protocolli sicuri, ecc.
- rendere sicuri / proteggere gli ambienti privati e pubblici mediante lo sviluppo di software di qualità, di 'firewall', programmi antivirus, sistemi di gestione dei diritti elettronici, crittazione, ecc.
- rendere sicura l'autenticazione degli utenti autorizzati, l'uso delle carte intelligenti, l'identificazione biometrica, le firme digitali, le tecnologie basate su ruoli, ecc.

Questo richiede un maggiore impegno per lo sviluppo di tecnologie per la sicurezza, nonché la cooperazione per raggiungere l'interoperabilità necessaria tra le soluzioni attraverso accordi in materia di norme internazionali.

È inoltre importante che gli eventuali futuri quadri concettuali per la sicurezza siano integrati nell'architettura complessiva, affinché già dall'inizio del processo di progettazione si affrontino le minacce e i punti vulnerabili. Questa strategia è antitetica rispetto agli approcci tradizionali basati su procedimento d'aggiunta successiva dei vari elementi, con cui si è cercato di colmare le lacune, sfruttate da una criminalità sempre più sofisticata.

Il programma nel settore delle tecnologie della società dell'informazione (TSI)<sup>18</sup> dell'Unione europea, segnatamente le attività riguardanti la sicurezza delle informazioni e delle reti, nonché le tecnologie volte a creare la fiducia,<sup>19</sup> forniscono un quadro per lo sviluppo di capacità e tecnologie per comprendere e affrontare le sfide che si profilano in relazione alla criminalità informatica. Tra queste tecnologie rientrano gli strumenti tecnici per la tutela contro la violazione dei diritti fondamentali alla riservatezza e alla protezione dei dati

---

<sup>18</sup> Il programma TSI è gestito dalla Commissione europea. S'inserisce nel 5° programma quadro per il periodo 1998 - 2002. Maggiori informazioni sono reperibili all'indirizzo <http://www.cordis.lu/ist>.

<sup>19</sup> Nell'azione chiave 2 - Nuovi metodi di lavoro e commercio elettronico.

personali e di altri diritti della persona e per combattere la criminalità informatica. Nel contesto del programma TSI è stata inoltre lanciata un'iniziativa sull'affidabilità, che contribuirà a diffondere la fiducia nelle infrastrutture d'informazione caratterizzate da un'elevata interoperabilità e nei sistemi incorporati in rete, promuovendo la percezione dell'affidabilità e le tecnologie atte a concretare quest'elemento. La cooperazione internazionale costituisce una parte integrante di tale iniziativa. Nell'ambito del programma TSI si sono instaurati dei rapporti operativi con DARPA e NSF ed è stata istituita, in collaborazione con il Dipartimento di Stato degli Stati Uniti, una task force UE/USA per la protezione dell'infrastruttura critica.<sup>20</sup>

Da ultimo, l'ottemperanza agli obblighi in materia di sicurezza imposti in particolare dalle direttive comunitarie sulla protezione dei dati personali<sup>21</sup>, contribuisce a migliorare la sicurezza delle reti e dell'elaborazione dati.

### **3. REATI CONNESSI AI SISTEMI INFORMATICI**

I moderni sistemi di informazione e comunicazione consentono di svolgere attività illecite da (e verso) qualsiasi punto del globo in qualsiasi momento. Non sono disponibili statistiche affidabili per quanto riguarda le reali dimensioni del fenomeno della criminalità connessa ai sistemi informatici. Il numero di casi di accesso indebito finora individuati e registrati probabilmente è di molto inferiore alla reale portata del problema. Molti di questi accessi indebiti non vengono individuati, in quanto gli amministratori e gli utilizzatori del sistema ne hanno una consapevolezza ed esperienza limitata; inoltre, molte imprese non sono disposte a divulgare i casi di abusi informatici per evitare pubblicità negativa e vulnerabilità nei confronti di attacchi futuri. Molte forze di polizia non tengono ancora statistiche in merito all'uso degli elaboratori e dei sistemi di comunicazione che sono oggetto di questi ed altri reati. Tuttavia è probabile che il numero di tali attività illecite possa aumentare con l'incremento dell'utilizzo dei computer e delle reti. È palese la necessità di raccogliere dati attendibili sulla portata della criminalità informatica.

Nella presente comunicazione si affrontano i reati connessi, in senso lato, ai sistemi informatici, intendendo con ciò ogni reato che comporti il ricorso alle tecnologie dell'informazione. Comunque, vi sono punti di vista diversi in merito alla definizione di "reato connesso ai sistemi informatici". I termini "reato informatico", "reato connesso ai sistemi informatici", "reato tramite alta tecnologia" e "reato telematico" sono spesso usati come sinonimi. È opportuno distinguere tra reati informatici specifici e reati di tipo convenzionale perpetrati con l'ausilio delle tecnologie informatiche. Un esempio di attualità è rappresentato dal settore delle dogane, in cui si riscontra che l'Internet viene impiegato per commettere reati contro la normativa doganale, quali il contrabbando, la contraffazione, ecc. Mentre i reati informatici specifici richiedono un aggiornamento delle definizioni riportate nei codici penali nazionali, i reati tradizionali perpetrati con l'ausilio di elaboratori rendono auspicabili una cooperazione e misure procedurali migliori.

---

<sup>20</sup> Sotto l'egida del gruppo consultivo paritetico istituito nell'ambito dell'accordo di cooperazione UE/USA nel campo della scienza e delle tecnologie.

<sup>21</sup> Cfr. l'articolo 4 della direttiva 97/66/CE (compreso l'obbligo d'informare gli interessati dei rischi residui in materia di sicurezza) e l'articolo 17 della direttiva 95/46/CE.

Tuttavia, tutti questi reati sono perpetrati grazie alla disponibilità di reti di informazione e comunicazione senza frontiere ed alla circolazione di dati immateriali ed estremamente labili. Ciò rende necessario un aggiornamento delle disposizioni esistenti in tema di attività illegali compiute nei confronti (o con l'utilizzo) di tali reti e sistemi.

Molti paesi hanno introdotto disposizioni che mirano a reprimere i reati connessi ai sistemi informatici. Negli Stati membri dell'Unione europea sono stati adottati numerosi atti normativi in materia; per quanto riguarda l'Unione europea, oltre a una decisione del Consiglio relativa alla pornografia su Internet, non esistono finora strumenti legislativi che disciplinino direttamente le violazioni connesse ai sistemi informatici, ma sono stati adottati numerosi strumenti legislativi indirettamente pertinenti.

Le questioni principali disciplinate dalla legislazione in materia di reati specificamente informatici a livello di Unione europea o di Stati membri sono le seguenti:

*Reati contro la riservatezza:* numerosi paesi hanno introdotto norme penali che affrontano gli illeciti attinenti la raccolta, la memorizzazione, l'alterazione, la divulgazione e diffusione di dati personali. A livello di Unione europea, sono state adottate due direttive che ravvicinano le disposizioni nazionali in materia di tutela della riservatezza con riguardo al trattamento dei dati personali<sup>22</sup>. L'articolo 24 della direttiva 95/46/CE statuisce espressamente che gli Stati membri sono tenuti ad adottare tutte le misure necessarie a garantire la piena attuazione delle disposizioni della direttiva, nonché ad irrogare sanzioni in caso di violazione delle disposizioni della normativa nazionale. Il diritto fondamentale alla riservatezza e il diritto fondamentale alla protezione dei dati sono sanciti inoltre dalla Carta dei Diritti fondamentali dell'Unione europea.

*Reati relativi ai contenuti:* la diffusione, soprattutto mediante Internet, della pornografia, e in particolare della pornografia infantile, di affermazioni razziste e di informazioni che incitano alla violenza inducono a chiedersi in quale misura tali atti possano essere affrontati con l'ausilio del diritto penale. La Commissione ha sostenuto la tesi che ciò che è illecito off-line dovrebbe essere tale anche on-line. L'autore o il fornitore dei contenuti<sup>23</sup> può essere chiamato a rispondere in sede penale. È stata adottata una decisione del Consiglio per combattere la pornografia infantile su Internet<sup>24</sup>. La responsabilità dei fornitori di servizi che fungono da intermediari, le cui reti o server vengono utilizzati per la trasmissione o la memorizzazione di informazioni relative a terzi è stata affrontata dalla direttiva sul commercio elettronico.

*Reati contro il patrimonio, accesso non autorizzato e sabotaggio:* numerosi paesi hanno introdotto norme relative ai reati contro il patrimonio specificamente connessi agli strumenti informatici e definiscono nuove fattispecie legate all'accesso non autorizzato ai sistemi informatici (ad esempio, la pirateria, il sabotaggio di elaboratori e la diffusione di virus

---

<sup>22</sup> Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e direttiva 97/66/CE del Parlamento europeo e del Consiglio, del 15 dicembre 1997, sul trattamento dei dati personali e sulla tutela della vita privata nel settore delle telecomunicazioni. L'art. 24 della Direttiva 95/46/CE obbliga gli Stati membri a stabilire sanzioni da applicare in caso di violazione delle disposizioni relative alla protezione dei dati.

<sup>23</sup> Il fornitore di contenuti non dovrebbe venire confuso con il fornitore del servizio.

<sup>24</sup> Decisione del Consiglio, del 29 maggio 2000, relativa alla lotta contro la pornografia infantile su Internet (GU L 138 del 9.6.2000, pag.1).

informatici, lo spionaggio informatico, la falsificazione informatica e la frode informatica<sup>25</sup>) e nuove modalità di violazione (ad esempio, manipolazioni di elaboratori invece di inganni a danno di individui). L'oggetto del reato è spesso immateriale, ad esempio, denaro in depositi bancari o programmi informatici. Attualmente, non esistono strumenti dell'Unione europea relativi a tali tipi di attività illegale. Per quanto riguarda la prevenzione, il regolamento recentemente adottato che emenda le precedenti disposizioni sui prodotti a duplice uso, liberalizza in notevole misura l'offerta di prodotti per la crittazione.

*Reati contro la proprietà intellettuale:* sono state adottate due direttive, relative alla tutela giuridica dei programmi per elaboratore e delle banche dati<sup>26</sup>, che trattano direttamente di temi inerenti alla società dell'informazione e prevedono l'adozione di sanzioni. Il Consiglio ha adottato una posizione comune concernente una proposta di direttiva sul diritto d'autore e sui diritti connessi nella società dell'informazione. Si prevede che tale direttiva sarà adottata all'inizio del 2001<sup>27</sup>. È necessario reprimere la violazione del diritto d'autore e dei diritti connessi, così come l'elusione delle misure tecnologiche volte a tutelare tali diritti. Per quanto riguarda la contraffazione e la pirateria, la Commissione presenterà, prima della fine del 2000, una comunicazione che tiene conto del processo di consultazione avviato con il Libro verde del 1998 e annuncia un piano d'azione in materia. Con l'aumentare dell'importanza commerciale di Internet, emergono nuove controversie legate ai nomi di dominio, come la registrazione abusiva di nomi di dominio (*cybersquatting*), l'accumulazione a fini speculativi di un gran numero di nomi di dominio (*warehousing*) e la riattribuzione controversa di nomi di dominio (*reverse hijacking*, fenomeno per cui le imprese di maggiori dimensioni sottraggono i nomi di dominio a concorrenti più piccoli): ovviamente vi è l'esigenza di predisporre regole e procedure che affrontino tali problemi<sup>28</sup>.

Occorre inoltre affrontare la problematica degli obblighi in materia fiscale. Per le operazioni commerciali in cui il destinatario della prestazione on-line di servizi telematici sia situato nell'Unione europea, gli obblighi fiscali sorgono nella giurisdizione ove si ritiene che il servizio sia fruito<sup>29</sup>. L'operatore che non adempia agli obblighi fiscali è passibile di sanzioni di diritto civile (ed in alcuni casi penali), varianti dal pignoramento dei conti bancari o dei

---

<sup>25</sup> I mezzi di comunicazione hanno dedicato grande spazio ai recenti attacchi che hanno provocato una interruzione del servizio con origine da più fonti ("*distributed denial of service*") su importanti siti web e alla diffusione del virus cosiddetto Lovebug. Tuttavia, è necessario contenere gli allarmismi. Gli attacchi che interrompono il servizio, sia deliberati che fortuiti, e i virus legati alla posta elettronica sono fenomeni presenti da molti anni. In passato si sono presentati gli esempi del "baco" Morris e del messaggio "Xmas-tree" dell'IBM. Esistono prodotti e procedure che consentono di affrontare tali problemi. Nella comunità degli utenti di Internet vi è inoltre un forte rapporto di collaborazione ai fini di limitare i danni provocati da tali eventi, come pure nel limitare gli abusi relativi all'invio in massa di messaggi elettronici (*spamming*).

<sup>26</sup> Direttiva 91/250/CEE del Consiglio, del 14 maggio 1991, relativa alla tutela giuridica dei programmi per elaboratore (GU L 122 del 17.5.1991, pagg. 42 – 46).

Direttiva 96/9/CE del Parlamento europeo e del Consiglio, dell'11 marzo 1996, relativa alla tutela giuridica delle banche di dati (GU L 77 del 27.3.1996, pagg. 20 – 28).

<sup>27</sup> Posizione comune definita dal Consiglio in vista dell'adozione di una direttiva del Parlamento europeo e del Consiglio sull'armonizzazione di taluni aspetti del diritto d'autore e dei diritti connessi nella società dell'informazione (CS/2000/9512).

<sup>28</sup> Comunicazione della Commissione al Consiglio e al Parlamento europeo L'organizzazione e la gestione di Internet - Aspetti di politica internazionale ed europea 1998-2000, aprile 2000, COM(2000) 202.

<sup>29</sup> La Commissione ha proposto una serie di modifiche al regime di imposta sul valore aggiunto all'interno della Comunità, allo scopo di chiarire la giurisdizione ai fini dell'imposizione fiscale (COM (2000)349 proposta di direttiva che modifica la direttiva 77/388/CEE per quanto riguarda il regime di imposta sul valore aggiunto applicabile a determinati servizi prestati tramite mezzi elettronici), attualmente al vaglio del Consiglio e del Parlamento. In taluni casi, tuttavia, il fornitore può essere assoggettato al pagamento dell'imposta, anche qualora questi non materialmente presente nella giurisdizione fiscale.

beni. Benché l'adempimento di tale obbligo su base volontaria sia sempre la soluzione preferibile, deve esistere in ultima analisi la possibilità di imporre l'ottemperanza forzata dell'obbligo fiscale.

La cooperazione tra le autorità fiscali costituisce l'elemento chiave per la realizzazione di tale obiettivo. Dando la possibilità ad alcuni di tutelare le proprie transazioni legali, si forniranno i medesimi mezzi a chi voglia proteggere i propri affari illeciti. Gli strumenti che consentono un commercio elettronico securizzato possono essere sfruttati anche a favore del traffico di droga. Sarà necessario individuare priorità e compiere le opportune scelte.

Nell'ambito della tutela delle vittime dei reati informatici occorre trattare problemi quali la responsabilità, i rimedi e il risarcimento, che si presentano ogniqualvolta sono commessi reati informatici. La fiducia non è determinata unicamente dall'impiego delle tecnologie appropriate, ma dipende anche dalle garanzie legali ed economiche offerte. Tali problemi devono essere esaminati per tutti i possibili reati informatici.

Sono necessari efficaci strumenti giuridici sostanziali e procedurali, armonizzati a livello globale, o almeno europeo, che tutelino le vittime della criminalità connessa ai sistemi informatici e assicurino i colpevoli alla giustizia. Al tempo stesso, le comunicazioni personali, la riservatezza, l'accesso e la divulgazione delle informazioni costituiscono diritti fondamentali delle moderne società democratiche. Per tale ragione, è opportuno dare priorità alla disponibilità e all'impiego di misure di prevenzione efficaci per ridurre la necessità di applicare provvedimenti che reprimano il fenomeno a posteriori. Le misure legislative relative ai reati connessi ai sistemi informatici devono mantenere un giusto equilibrio tra queste importanti esigenze.

#### **4. QUESTIONI DI DIRITTO SOSTANZIALE**

Il ravvicinamento delle disposizioni di diritto sostanziale nel campo della criminalità ad alta tecnologia offrirà un livello minimo di tutela delle vittime di reati telematici (ad esempio, le vittime della pornografia infantile), contribuirà a soddisfare la condizione che un'attività debba costituire un reato in entrambi i paesi perché possa essere richiesta l'assistenza giudiziaria reciproca in un'indagine penale (clausola della duplice perseguibilità) e creerà maggiore chiarezza per gli operatori del settore (in merito, ad esempio, alla nozione di contenuto illecito).

Infatti, successivamente al Vertice del Consiglio europeo di Tampere, dell'ottobre 1999<sup>30</sup>, tra le iniziative da attuare da parte dell'Unione europea è stato inserito uno strumento giuridico dell'Unione inteso a ravvicinare il diritto penale sostanziale nel campo della criminalità connessa ai sistemi informatici. Il Vertice ha incluso la criminalità ad alta tecnologia in un ristretto elenco di settori in cui è necessario uno sforzo comune per concordare definizioni di fattispecie, condizioni di perseguibilità e trattamento sanzionatorio. Ciò è riportato nella raccomandazione n. 7 relativa alla strategia dell'Unione europea per il nuovo millennio sulla prevenzione e il controllo della criminalità organizzata, adottata dal Consiglio GAI nel marzo del 2000<sup>31</sup> e fa parte anche del programma di lavoro della Commissione per

---

<sup>30</sup> <http://db.consilium.eu.int/it/Info/eurocouncil/index.htm>.

<sup>31</sup> Prevenzione e controllo della criminalità organizzata - Strategia dell'Unione europea per il nuovo millennio (GU C 124, 3.5.2000).

l'anno 2000 e del quadro di controllo per la creazione di uno spazio di "libertà, sicurezza e giustizia", elaborato dalla Commissione e adottato dal Consiglio GAI il 27 marzo 2000<sup>32</sup>.

La Commissione ha seguito l'attività del Consiglio d'Europa concernente la convenzione sulla criminalità informatica. Nell'attuale progetto di convenzione figurano quattro categorie di reati penali: 1) reati contro la riservatezza, l'integrità e la disponibilità di dati e sistemi informatici; 2) reati connessi ai sistemi informatici; 3) reati connessi ai contenuti; 4) reati connessi a violazioni dei diritti d'autore e dei diritti correlati.

Il ravvicinamento della normativa all'interno dell'Unione europea potrebbe spingersi oltre la portata della convenzione del Consiglio d'Europa, che rappresenterà il livello minimo di armonizzazione internazionale, e divenire operativo entro un termine più breve di quello previsto per l'entrata in vigore della suddetta convenzione<sup>33</sup>. In tal modo la criminalità informatica farebbe il suo ingresso tra le materie disciplinate dalla legislazione dell'Unione e verrebbero introdotti meccanismi per garantire il rispetto delle disposizioni comunitarie.

La Commissione ritiene di importanza fondamentale che l'Unione europea sia in grado di agire in maniera efficace, segnatamente contro la pornografia infantile su Internet, e esprime quindi il proprio apprezzamento nei confronti della decisione del Consiglio che mira a contrastare tale fenomeno, ma condivide il parere del Parlamento europeo, secondo cui sono necessarie ulteriori azioni intese a ravvicinare le legislazioni nazionali. Entro la fine del corrente anno, la Commissione intende presentare una proposta di decisione quadro che comprenda norme per il ravvicinamento delle legislazioni e sanzioni contro la pornografia infantile in rete.<sup>34</sup>

Conformemente a quanto stabilito nelle conclusioni del Consiglio di Tampere, la Commissione presenterà una proposta legislativa nel quadro del Titolo VI del trattato dell'Unione europea intesa a ravvicinare le nozioni di reato penale in relazione alla criminalità ad alta tecnologia. Tale proposta si baserà sui progressi compiuti nell'ambito del Consiglio d'Europa e tratterà in particolare l'esigenza di ravvicinare le normative nazionali in materia di accesso abusivo a sistemi informatici e di attacchi che provocano l'interruzione dei servizi. La proposta comprenderà delle definizioni uniformi per l'Unione europea in questo settore. Il testo potrebbe inoltre avere una portata maggiore del progetto di convenzione del Consiglio d'Europa, in quanto garantirebbe l'irrogazione di una sanzione penale minima in tutti gli Stati membri per i casi gravi di accesso abusivo ai sistemi informatici e d'interruzione dei servizi.

Inoltre, la Commissione analizzerà le possibilità d'azione nella lotta al razzismo e alla xenofobia su Internet, nella prospettiva di una proposta di decisione quadro del Consiglio nell'ambito del Titolo VI del trattato dell'Unione europea concernente le attività razziste e xenofobiche in rete e non. Si terrà conto dell'imminente valutazione relativa all'attuazione data dagli Stati membri all'azione comune del 15 luglio 1996 per la lotta contro il razzismo e la xenofobia<sup>35</sup>. L'azione comune costituisce il primo passo verso il ravvicinamento delle

---

<sup>32</sup> [http://Europa.eu.int/comm/dgs/justice\\_home/index\\_it.htm](http://Europa.eu.int/comm/dgs/justice_home/index_it.htm).

<sup>33</sup> La convenzione del Consiglio d'Europa entrerà in vigore solo successivamente alla ratifica.

<sup>34</sup> Tale iniziativa si inserisce in un pacchetto di proposte che trattano anche temi più ampi, legati allo sfruttamento sessuale dei minori e al traffico di esseri umani, come annunciato nella comunicazione della Commissione, del dicembre 1998, sulla tratta di esseri umani. Il testo della proposta di decisione quadro è allegato alla comunicazione della Commissione al Consiglio e al Parlamento europeo relativa alla lotta alla degli esseri umani e allo sfruttamento sessuale dei minori: due proposte di decisioni quadro, pubblicate parallelamente alla presente comunicazione.

<sup>35</sup> GU L 185, 24.7.1996, pagg. 5-7. Reperibile anche al sito della Rete giudiziaria europea: <http://ue.eu.int/ejn/index.htm>.

disposizioni penali in materia di razzismo e xenofobia; occorre tuttavia ancora impegnarsi per un ulteriore ravvicinamento delle normative all'interno dell'Unione europea. L'importanza e il carattere delicato di queste problematiche sono stati messi in luce dalla decisione di un tribunale francese, in data 20 novembre 2000, che ha ingiunto a Yahoo di impedire l'accesso degli utenti francesi ai siti che commercializzano cimeli nazisti<sup>36</sup>

Infine, la Commissione esaminerà le modalità da seguire per migliorare l'efficacia degli sforzi contro il traffico di stupefacenti via Internet, la cui importanza viene riconosciuta dalla strategia antidroga 2000-2004 dell'Unione europea, adottata dal Consiglio europeo di Helsinki<sup>37</sup>.

## **5. QUESTIONI DI DIRITTO PROCESSUALE**

Le questioni inerenti alla procedura penale balzano in primo piano a livello nazionale e internazionale per la natura stessa dei reati penali connessi ai sistemi informatici, che coinvolge via via differenti sovranità, giurisdizioni e legislazioni. La velocità, mobilità e flessibilità dei reati connessi ai sistemi informatici mettono a dura prova le attuali norme di procedura penale.

Il ravvicinamento dei poteri nell'ambito del diritto processuale penale migliorerà la tutela delle vittime, in quanto garantisce che gli organi preposti all'applicazione della legge abbiano i poteri necessari per condurre indagini sui reati sul territorio di loro competenza, e garantirà inoltre che possano rispondere rapidamente ed efficacemente alle richieste di cooperazione provenienti da altri paesi.

È inoltre importante che si provveda affinché le misure adottate sulla base del diritto penale, che di norma sono di competenza degli Stati membri e che rientrano nel Titolo VI del trattato dell'Unione europea, siano conformi alle disposizioni del diritto comunitario. In particolare, la Corte di giustizia ha costantemente affermato che dette disposizioni legislative non possono porre in essere discriminazioni nei confronti di soggetti cui il diritto comunitario attribuisce il diritto alla parità di trattamento né limitare le libertà fondamentali garantite dal diritto comunitario<sup>38</sup>. Gli eventuali nuovi poteri in materia di applicazione della legge devono essere valutati alla luce del diritto comunitario e del loro impatto sulla riservatezza.

### **5.1. Intercettazione di comunicazioni**

Nell'Unione europea vige il principio generale della segretezza delle comunicazioni (e dei relativi dati circa il traffico). Le intercettazioni sono illecite salvo se autorizzate dalla legge, nel caso siano necessarie in casi specifici per scopi limitati. Questo principio discende dall'articolo 8 della Convenzione europea dei diritti dell'uomo, cui fa riferimento l'articolo 6 del Trattato sull'Unione europea, e più in particolare dalle direttive 95/46/CE e 97/66/CE.

---

<sup>36</sup> Tribunal de Grande Instance de Paris, Ordonnance de Référé emessa il 20 novembre 2000, n. RG 00/05308.

<sup>37</sup> Piano d'azione dell'Unione europea in materia di lotta contro la droga (2000-2004) - COM(1999) 239 def. [http://europa.eu.int/comm/justice\\_home/unit/drogue\\_en.htm](http://europa.eu.int/comm/justice_home/unit/drogue_en.htm).

<sup>38</sup> Causa C-274/96 Bickel & Franz (1998), Racc. pag. I-7637, par. 17; causa C-186/87 Cowan (1989), Racc. pag. 195, par. 19. In particolare, le misure amministrative o repressive non devono esulare dai limiti di quanto è strettamente necessario, le modalità di controllo non devono essere concepite in modo da limitare la libertà voluta dal trattato e non è lecito comminare in proposito sanzioni talmente sproporzionate rispetto alla gravità dell'infrazione da risolversi in un ostacolo a tale libertà (causa C-203/80 Casati (1981) Racc. 2595, par. 27).

Tutti gli Stati membri sono dotati di un quadro normativo che consente a chi ha il compito di garantire il rispetto della legge di ottenere l'ordine del giudice (o nel caso di due Stati membri, un mandato autorizzato personalmente da un ministro) per effettuare intercettazioni di comunicazioni sulle reti pubbliche di telecomunicazioni.<sup>39</sup> Detta normativa, che deve essere conforme al diritto comunitario nella misura in cui questo sia d'applicazione, prevede misure di salvaguardia del diritto fondamentale dei cittadini alla tutela della vita privata, quali ad esempio la limitazione dell'utilizzo di intercettazioni alle indagini relative a reati gravi, il requisito che le intercettazioni effettuate dagli inquirenti nei confronti di individui siano strettamente necessarie e proporzionate, o la garanzia che l'interessato sia informato dell'intercettazione, non appena ciò non interferisca con le indagini. In numerosi Stati membri, le disposizioni relative alle intercettazioni impongono agli operatori di telecomunicazioni che offrono un servizio pubblico di prevedere strutture per consentire di intercettare le comunicazioni. Nel 1995, è stata adottata una risoluzione del Consiglio che mirava a coordinare i requisiti relativi alle intercettazioni<sup>40</sup>.

Gli operatori di rete tradizionali, in particolare quelli che offrono servizi vocali, hanno già da tempo stabilito con le autorità preposte al rispetto della legge rapporti di collaborazione operativa per agevolare l'intercettazione legale delle comunicazioni. La liberalizzazione delle telecomunicazioni e la crescita esponenziale degli utilizzatori di Internet hanno spinto a inserirsi nel mercato numerosi nuovi operatori, che si sono trovati ad affrontare per la prima volta il problema dei requisiti per l'intercettazione. Di conseguenza, sarà necessario avviare un dialogo tra lo Stato e gli operatori del settore, nonché tutte le parti interessate - comprese le autorità di controllo preposte alla protezione dei dati - su tutte le questioni che coinvolgono le regole, la fattibilità tecnica, l'allocazione dei costi e l'impatto commerciale.

L'avvento di nuove tecnologie rende indispensabile la collaborazione degli Stati membri, se questi vogliono conservare la possibilità di effettuare intercettazioni legali delle comunicazioni. La Commissione ritiene che, qualora gli Stati membri introducano nuovi requisiti tecnici in materia di intercettazione per gli operatori di telecomunicazioni e i fornitori di servizi su Internet, tali specifiche dovrebbero essere coordinate a livello internazionale, per prevenire una distorsione del mercato unico, al fine di minimizzare i costi a carico degli operatori del settore e per garantire l'ottemperanza alle disposizioni in materia di riservatezza e protezione dei dati. Tali requisiti dovrebbero essere il più possibile pubblici e trasparenti e non dovrebbero causare difficoltà alle infrastrutture delle comunicazioni.

---

<sup>39</sup> Due Stati membri non consentono l'uso delle intercettazioni di comunicazioni come materiale probatorio nei processi penali.

<sup>40</sup> Risoluzione del Consiglio del 17 gennaio 1995 sull'intercettazione legale delle telecomunicazioni (GU C 329 del 4.11.1996, pagg. 1- 6). L'allegato contiene un elenco di condizioni per l'intercettazione legale da parte degli inquirenti, delle quali gli Stati membri dovevano tenere conto nel definire ed attuare politiche e misure nazionali pertinenti. Nel 1998, la presidenza austriaca ha proposto una risoluzione del Consiglio dell'Unione europea volta ad estendere l'ambito di applicazione della risoluzione del 1995 alle nuove tecnologie, inclusi Internet e le comunicazioni satellitari. Tale tema ha costituito argomento di dibattito in due commissioni parlamentari, la commissione "Libertà pubbliche e affari interni" e la commissione giuridica e per i diritti dei cittadini, che sono giunte a conclusioni difformi. La prima ha reputato che tale risoluzione rappresentasse una chiarificazione e un aggiornamento della precedente e che quindi fosse accettabile. La seconda si è dimostrata fortemente critica, a causa delle potenziali violazioni dei diritti dell'uomo e dei costi per gli operatori, respingendo la proposta del Consiglio e chiedendo alla Commissione di preparare una nuova proposta successivamente all'entrata in vigore del trattato di Amsterdam. La proposta di risoluzione non è stata presa in considerazione né dal Consiglio né dai suoi gruppi di lavoro negli ultimi mesi.

Nel contesto della convenzione relativa all'assistenza giudiziaria in materia penale tra gli Stati membri dell'Unione europea,<sup>41</sup> sono stati concordati criteri per facilitare la cooperazione in materia di intercettazioni legali<sup>42</sup>. La convenzione comprende disposizioni sull'intercettazione delle comunicazioni telefoniche via satellite<sup>43</sup> e delle comunicazioni di una persona fisica che si trovi nel territorio di un altro Stato membro.<sup>44</sup> La Commissione ritiene che le disposizioni in materia di intercettazione contenute nella Convenzione relativa all'assistenza giudiziaria rappresentino lo strumento più avanzato che è possibile definire allo stato attuale. Il testo di tale documento è neutrale nei confronti delle tecnologie, e prima di poter programmare eventuali miglioramenti se ne dovrà verificare il funzionamento sul piano pratico. La Commissione analizzerà la sua applicazione in collaborazione con gli Stati membri, gli operatori del settore, gli utilizzatori e le autorità di controllo competenti in materia di protezione dei dati per garantire che le iniziative pertinenti siano efficaci, trasparenti ed equilibrate.

L'impiego abusivo ed indiscriminato delle strutture di intercettazione, soprattutto a livello internazionale, è suscettibile di sollevare problemi di rispetto dei diritti umani e di minare la fiducia dei cittadini nella società dell'informazione. La Commissione ha constatato con grande preoccupazione che sono stati segnalati casi di presunti abusi dei mezzi di intercettazione.<sup>45</sup>

## **5.2. Conservazione dei dati relativi alle comunicazioni**

Nel corso delle indagini e delle azioni intese a reprimere le violazioni penali legate all'impiego delle reti di telecomunicazione, tra cui Internet, le autorità preposte all'applicazione della legge si servono spesso di dati relativi al traffico, qualora vengano conservati dai fornitori di servizi soprattutto a fini di fatturazione. Tuttavia, dato che il costo di una comunicazione dipende sempre meno dalla destinazione e dalla distanza e i fornitori di servizi adottano sempre più spesso tariffe forfettarie, verrà meno l'esigenza di conservare i dati sul traffico a fini di fatturazione. Le autorità preposte all'applicazione della legge temono

---

<sup>41</sup> GU C 197 del 12.7.2000, pag. 1. La Convenzione è stata adottata il 29 maggio 2000. Le disposizioni relative alle intercettazioni si applicano solo agli Stati membri dell'Unione europea e non ai paesi terzi.

<sup>42</sup> La Convenzione contempla delle clausole minime di salvaguardia concernenti la tutela della sfera privata e la protezione dei dati.

<sup>43</sup> L'obiettivo iniziale dei negoziati era di fornire i mezzi per effettuare intercettazioni nei confronti di persone che si servono di telefoni satellitari nel territorio dello Stato membro che effettua l'intercettazione. Tecnicamente, il punto critico in cui si compie l'intercettazione è la stazione terrestre di comunicazione via satellite. Era quindi necessario ricorrere all'assistenza tecnica dello Stato membro nel quale si trova la stazione satellitare di terra. La convenzione prevede due soluzioni alternative a tale problema: un procedimento accelerato di assistenza giudiziaria reciproca che comprenda specifiche richieste di assistenza allo Stato membro nel cui territorio si trova il ricevitore di terra, e un'alternativa tecnica basata sull'accesso remoto al ricevitore satellitare di terra da parte dello Stato membro che effettua l'intercettazione, senza necessità di richiesta specifica per i singoli casi.

<sup>44</sup> La convenzione istituisce anche un quadro normativo relativamente alle richieste di intercettare le comunicazioni di una persona sul territorio di un altro Stato membro (lo Stato membro richiesto). In tal caso, lo Stato membro che compie l'intercettazione e quello richiesto devono entrambi conformarsi alle condizioni previste dalla loro normativa nazionale. Infine, la convenzione stabilisce norme per situazioni nelle quali lo Stato membro che intercetta ha la possibilità di intercettare le comunicazioni di una persona che si trova nel territorio di un altro Stato membro senza la necessità di richiedere assistenza tecnica da quest'ultimo Stato.

<sup>45</sup> Durante un'udienza pubblica del Parlamento europeo è stata presentata una lunga relazione, redatta dall'onorevole Campbell e basata su ampia documentazione, riguardante una rete di intercettazione dei servizi segreti detta ECHELON ([http://www.gn.apc.org/duncan/stoa\\_cover.htm](http://www.gn.apc.org/duncan/stoa_cover.htm)). Nella relazione si sostiene che ECHELON è stato creato per ragioni di sicurezza nazionale, ma è stato utilizzato anche a fini di spionaggio industriale. Il Parlamento europeo ha istituito una commissione temporanea incaricata di compiere uno studio sul tema e di presentare entro un anno una relazione alla sessione plenaria.

che in tal modo verrà a mancare materiale potenzialmente utile per le indagini penali e pertanto sostengono la necessità di obbligare i fornitori di servizi a conservare i dati sul traffico per un lasso di tempo minimo, così che tali dati possano venire utilizzati per fini di applicazione della legge.<sup>46</sup>

Conformemente alle direttive dell'Unione europea sulla protezione dei dati, ossia ai principi di limitazione di carattere generale della direttiva 95/46/CE e alle disposizioni più specifiche della direttiva 97/66/CE, i dati sul traffico devono essere eliminati o resi anonimi immediatamente dopo la fornitura del servizio di telecomunicazioni, salvo qualora la loro conservazione sia necessaria a fini della fatturazione. In generale, ai fornitori di servizi che applicano tariffe forfettarie o concedono accesso gratuito alle telecomunicazioni non è consentito conservare i dati sul traffico.

Ai sensi delle direttive dell'Unione europea sulla protezione dei dati, gli Stati membri hanno la facoltà di adottare misure legislative che restringano l'ambito dell'obbligo di eliminare tali dati qualora ciò costituisca un provvedimento essenziale ad esempio per prevenire, investigare, accertare e perseguire i reati penali o l'uso non autorizzato del sistema di telecomunicazioni.<sup>47</sup>

Tuttavia, qualsiasi misura legislativa a livello nazionale che preveda eventualmente la conservazione dei dati sul traffico per la repressione della criminalità dovrebbe rispettare alcune condizioni: le misure proposte devono essere adeguate, necessarie e rispettose del principio di proporzionalità, conformemente al diritto comunitario e al diritto internazionale, compresa la direttiva 97/66/CE, la direttiva 95/46/CE, la Convenzione europea per la salvaguardia dei diritti dell'uomo del 4 novembre 1950 e la Convenzione del Consiglio d'Europa, del 28 gennaio 1981, sulla protezione delle persone con riferimento al trattamento automatizzato dei dati di carattere personale. Il rispetto di tali principi è particolarmente importante per i provvedimenti intesi a prevedere la conservazione abituale dei dati relativi a una grande percentuale della popolazione.

Alcuni Stati membri stanno introducendo norme giuridiche che impongono o consentono ai fornitori di servizi di conservare, dopo la prestazione del servizio, alcune categorie di dati relativi al traffico, non necessari a fini di fatturazione, ma ritenute utili per indagini penali.

L'ampiezza e la forma di tali iniziative variano in maniera notevole, ma esse hanno in comune la concezione per cui le autorità preposte all'applicazione della legge dovrebbero avere accesso a una maggior quantità di dati di quella disponibile nel caso in cui i fornitori di servizi trattassero esclusivamente i dati necessari per offrire il servizio. La Commissione sta esaminando tali misure alla luce del diritto comunitario in vigore.

Il Parlamento europeo è sensibile al tema della riservatezza e in generale ha sempre preso posizione a favore di una rigorosa tutela dei dati personali. Tuttavia, nel corso delle discussioni sulla lotta alla pornografia infantile su Internet, il Parlamento europeo ha espresso un parere a sostegno dell'obbligo generale di mantenere i dati sul traffico per un periodo di tre mesi.<sup>48</sup>

---

<sup>46</sup> Compresa le indagini penali relative a casi non legati ai sistemi informatici e telematici, ma nei quali i dati di tali sistemi potrebbero essere utili per perseguire il reato.

<sup>47</sup> Art. 14 della direttiva 97/66/CE ed art. 13 della direttiva 95/46/CE.

<sup>48</sup> Risoluzione legislativa recante il parere del Parlamento europeo sul progetto di azione comune, adottata dal Consiglio sulla base dell'articolo K.3 del trattato sull'Unione europea per la lotta contro la pornografia infantile su Internet, emendamento 17 (GU C 219 del 30.7.1999, pagg. 68 segg., pag. 71).

Ciò dimostra l'importanza del contesto in cui viene discusso un tema delicato come quello della conservazione dei dati sul traffico e le dimensioni del problema che i politici si trovano ad affrontare alla ricerca di un giusto equilibrio tra esigenze in conflitto.

La Commissione reputa che qualsiasi soluzione al complesso problema della conservazione dei dati sul traffico dovrebbe avere valide motivazioni, essere rispettosa del principio di proporzionalità e garantire un giusto equilibrio tra gli interessi in gioco. Solo una strategia che combini le competenze specifiche e le capacità delle autorità nazionali, degli operatori del settore, delle autorità garanti della tutela dei dati e degli utilizzatori consentirà di conseguire questi obiettivi. Sarebbe auspicabile che tutti gli Stati membri adottassero una strategia coerente in relazione a questa complessa problematica, per conseguire gli obiettivi di efficacia e di proporzionalità e, allo stesso tempo, evitare che le autorità incaricate di far osservare le norme e la comunità di Internet si trovino ad affrontare un mosaico di contesti tecnici e giuridici eterogenei.

Gli elementi da tenere in considerazione sono molteplici. Da un lato, le autorità garanti della protezione dei dati hanno affermato che il mezzo migliore per ridurre rischi inaccettabili in materia di riservatezza, pur nella salvaguardia delle esigenze delle autorità giudiziarie, consiste nell'evitare che i dati sul traffico siano conservati esclusivamente a fini giudiziari.<sup>49</sup> Le autorità preposte all'osservanza della legge hanno dichiarato che, a loro parere, è necessario conservare almeno una minima quantità di dati sul traffico per il lasso di tempo sufficiente ad agevolare le indagini penali.

Benché sia nell'interesse dell'industria informatica cooperare nella lotta contro reati come la pirateria e la frode informatica, gli operatori non dovrebbero essere costretti a prendere provvedimenti eccessivamente onerosi. Occorre analizzare accuratamente l'incidenza economica delle eventuali misure e ponderarne l'efficacia ai fini della lotta alla criminalità telematica, onde evitare che l'uso dell'Internet diventi più costoso e meno abbordabile per gli utilizzatori. Si dovrebbero garantire adeguati sistemi di sicurezza per i dati conservati.

Ad ogni modo, gli operatori del settore avranno un ruolo di primo piano da svolgere, su base volontaria, nel processo di creazione di una società dell'informazione più sicura. Gli utilizzatori dovrebbero avere fiducia nella sicurezza della società dell'informazione e sentirsi protetti nei confronti della criminalità e delle violazioni della propria sfera privata.

La Commissione sostiene pienamente e incoraggia un dialogo costruttivo tra autorità preposte all'applicazione della legge, gli operatori del settore, le autorità competenti in materia di protezione dei dati e le associazioni per la tutela dei consumatori, nonché altre eventuali parti interessate. Nel quadro del Forum proposto a livello di Unione europea (cfr. punto 6.4 della presente comunicazione), la Commissione inviterà tutte le parti interessate a inserire tra le proprie priorità una discussione approfondita su tale complesso problema, per trovare congiuntamente soluzioni adeguate, equilibrate e proporzionate, nel pieno rispetto dei diritti

---

<sup>49</sup> “Le attività generali di esplorazione o sorveglianza su vasta scala devono essere vietate...il mezzo più efficace per limitare inaccettabili pericoli alla riservatezza nella salvaguardia delle esigenze delle autorità giudiziarie consiste nell'evitare che i dati sul traffico siano mantenuti esclusivamente a fini giudiziari, e che le leggi nazionali costringano gli operatori delle telecomunicazioni, i servizi di telecomunicazione e i fornitori di servizi Internet a mantenere dati sul traffico per un periodo di tempo superiore a quello necessario ai fini di fatturazione.” Raccomandazione 3/99 del 7 settembre 1999 del Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito a norma dell'articolo 29, [http://europa.eu.int/comm/internal\\_market/en/media/dataprot/wpdocs/index.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm)

fondamentali relativi alla riservatezza e alla protezione dei dati<sup>50</sup>. In base ai risultati di tale lavoro, la Commissione potrà valutare la necessità di azioni legislative o non legislative a livello dell'Unione europea.

### 5.3. Accesso e utilizzo anonimi

Gli esperti in tema di applicazione della legge hanno espresso il timore che garantendo l'anonimato, ci si trovi impossibilitati a chiamare a rispondere i responsabili di illeciti e quindi gravemente impediti nell'assicurare alla giustizia taluni criminali. L'utilizzo anonimo della telefonia mobile è possibile in alcuni paesi, mediante l'impiego di schede prepagate (e non in altri). Per quanto riguarda Internet, alcuni fornitori di accesso e di servizi - come i servizi di redistribuzione di posta elettronica e gli Internet café - offrono accesso e utilizzo anonimo della rete. L'anonimato è anche favorito in una certa misura dal sistema di indirizzamento dinamico di Internet, per il quale gli indirizzi non sono assegnati agli utenti su base permanente, ma solo per la durata di una sessione di collegamento.

Nel corso dei dibattiti con la Commissione, alcuni rappresentanti degli operatori del settore non si sono dichiarati favorevoli all'anonimato totale, in parte per ragioni di sicurezza interna, ma anche di lotta alle frodi e di tutela dell'integrità delle reti. Il London Internet Exchange ha menzionato le sue linee direttrici sulle migliori pratiche, che si sono rivelate utili nel Regno Unito.<sup>51</sup> Tuttavia, altri rappresentanti degli operatori del settore ed esperti privati sostengono che senza l'anonimato non sia possibile garantire la tutela dei diritti fondamentali.

Il Gruppo Art. 29 per la tutela delle persone con riguardo al trattamento dei dati ha emesso una raccomandazione sul tema dell'utilizzo anonimo di Internet<sup>52</sup>, nella quale il problema dell'anonimato sulla rete viene definito come fonte di enormi incertezze per i governi e per le organizzazioni internazionali. Da un lato, la possibilità di celare la propria identità è di importanza vitale per preservare i diritti fondamentali di riservatezza e di libera espressione sulle reti informatiche e telematiche; dall'altro, l'opportunità di partecipare e di comunicare on-line senza rivelare la propria identità ostacola le iniziative adottate a favore di altri settori chiave delle politiche pubbliche, come la lotta contro i contenuti nocivi e illeciti, contro le frodi finanziarie o le violazioni dei diritti d'autore. Ovviamente, tali evidenti conflitti tra obiettivi politici differenti non rappresentano una novità. Nell'ambito dei mezzi di comunicazione off-line più tradizionali, come l'invio per corrispondenza di lettere e pacchi, il telefono, i giornali o la diffusione radiofonica o televisiva, è stato raggiunto un equilibrio tra questi obiettivi. I politici di oggi devono individuare in che modo sia possibile ottenere che nel nuovo contesto del cyberspazio venga salvaguardata questa strategia di equilibrio, che garantisce i diritti fondamentali pur consentendo limitazioni proporzionate di tali diritti in circostanze specifiche. Un elemento fondamentale di tale equilibrio consisterà nel definire in quale misura e con quali limiti il singolo potrà intervenire on-line in maniera anonima.

Nella dichiarazione conclusiva della conferenza ministeriale di Bonn sulle reti di informazione globali del 6-8 luglio 1997, si è affermato che, in linea di principio, nei casi in cui l'utente abbia la possibilità di rimanere anonimo off-line, dovrebbe essergli garantita tale

---

<sup>50</sup> In base a quanto stabilito nella Convenzione europea sui diritti dell'uomo (articolo 8, diritto alla riservatezza), nella Carta sui diritti fondamentali dell'Unione europea, nel trattato dell'Unione europea e nelle direttive concernenti la protezione dei dati.

<sup>51</sup> <http://www.linx.net/noncore/bcp>.

<sup>52</sup> Gruppo di lavoro per la tutela delle persone con riguardo al trattamento dei dati personali. Raccomandazione 3/97, Anonimato su Internet. Adottato dal Gruppo di lavoro il 3 dicembre 1997. [http://europa.eu.int/comm/internal\\_market/en/media/dataprot/wpdocs/index.htm](http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/index.htm).

opportunità anche on-line. Pertanto, da più parti si concorda che l'attività sulle reti dovrebbe essere disciplinata dai medesimi principi giuridici fondamentali applicati in altri contesti. Internet non è un'isola di anarchia nella quale non vigono le regole della società. Al tempo stesso, tuttavia, la capacità dei governi e delle pubbliche autorità di limitare i diritti degli individui e di sorvegliare i comportamenti potenzialmente illeciti sulle reti pubbliche non dovrebbe essere superiore alla capacità di cui tali istanze si avvalgono nel mondo esterno, off-line. Anche nel cyberspazio è necessario applicare la condizione per cui le restrizioni ai diritti e alle libertà fondamentali devono essere adeguatamente giustificate, necessarie e proporzionate rispetto ad altri obiettivi di politica pubblica.

Nella raccomandazione del Gruppo di tutela istituito in base all'articolo 29 vengono espresse indicazioni dettagliate sulle modalità per raggiungere tali obiettivi in alcuni casi specifici (ad esempio, per quanto riguarda la posta elettronica, i newsgroups ecc.).<sup>53</sup> La Commissione condivide le opinioni espresse dal Gruppo di lavoro.

#### **5.4. Cooperazione concreta a livello internazionale**

Negli ultimi tempi, le operazioni congiunte di applicazione della legge condotte a livello mondiale, quali l'operazione 'Starburst' e l'operazione 'Cathedral' contro i circuiti pedofili, hanno evidenziato il valore dell'azione internazionale coordinata tra le autorità giudiziarie e gli organismi di polizia, sia mediante scambio d'informazioni nella fase preliminare sia evitando che gli altri membri del circuito abbiano sentore dell'imminenza di arresti e sequestri giudiziari. L'Internet si è dimostrato un prezioso ed efficace strumento, ai fini delle indagini di polizia e di finanza, laddove è usato per commettere reati tradizionali, quali la contraffazione e il contrabbando. Dall'altro lato, le suddette operazioni hanno inoltre messo a nudo le principali difficoltà giuridiche ed operative incontrate dagli organismi preposti all'applicazione della legge e dalle autorità giudiziarie nel condurre tali azioni, quali la raccolta di materiale probatorio o le rogatorie, l'identificazione delle vittime e il ruolo delle organizzazioni intergovernative competenti in questioni di polizia (segnatamente Interpol ed Europol).

Sul piano delle misure concrete di cooperazione internazionale, le reti internazionali per lo scambio di informazioni stanno assumendo un ruolo sempre più importante per le forze di polizia e le autorità doganali.

Nell'ambito del G8 è stata istituita una rete di punti di contatto, già operativa, tra autorità preposte all'applicazione della legge per lo scambio d'informazioni, attiva 24 ore al giorno e 7 giorni alla settimana. Il suo principale obiettivo è ricevere e rispondere a richieste urgenti di cooperazione in casi che comportano il reperimento di materiale probatorio mediante mezzi o supporti elettronici. La rete è stata utilizzata con successo in diverse operazioni. Il Consiglio GAI del 19 marzo 1998 ha sottoscritto i 10 principi per la lotta contro la criminalità ad alta tecnologia adottati dal G8 ed ha esortato gli Stati membri dell'UE che non partecipano al G8 ad aderire alla rete<sup>54</sup>. I predetti punti di contatto dovrebbero cooperare direttamente, integrando le attuali strutture di assistenza giudiziaria e i canali di comunicazioni.<sup>55</sup>

---

<sup>53</sup> [http://europa.eu/int/comm/internal\\_market/en/media/dataprot/wpdocs/index.htm](http://europa.eu/int/comm/internal_market/en/media/dataprot/wpdocs/index.htm).

<sup>54</sup> Oltre ai membri del G8, alla suddetta rete hanno aderito finora cinque Stati membri dell'UE.

<sup>55</sup> In occasione della Conferenza mondiale contro lo sfruttamento commerciale dei minori, svoltasi a Stoccolma il 28 agosto 1996 si è proposto di far partecipare l'INTERPOL alle reti summenzionate. La decisione del Consiglio dell'Unione europea relativa alla lotta contro la pornografia infantile su Internet contempla anch'essa la partecipazione di Europol in questo campo.

La creazione di una tale rete è inoltre contemplata nel progetto di convenzione del Consiglio d'Europa. Anche nella decisione del Consiglio sulla lotta contro la pornografia infantile su Internet e nella posizione comune dell'UE sul progetto di convenzione del Consiglio d'Europa sulla cybercriminalità<sup>56</sup>, nonché nella decisione del Consiglio in cui ha sottoscritto il piano d'azione del G8<sup>57</sup>, si fa riferimento ad una rete di contatti attiva 24 ore su ventiquattro, 7 giorni su sette, ma finora nell'ambito UE non sono ancora state prese iniziative concrete specifiche.

La Commissione ritiene che, vista l'esigenza di disporre di adeguate conoscenze specialistiche e di condurre azioni tempestive in questo settore, si dovrebbe dare immediatamente esecuzione alle intenzioni del Consiglio. Affinché tuttavia tale rete abbia successo, occorre del personale preparato sia sul piano giuridico che tecnico, il che presuppone un'opportuna formazione.

Un'analoga esigenza di intensificare la cooperazione e lo scambio di informazioni è sentita anche dalle autorità doganali. Si dovrebbero rafforzare le attuali forme di cooperazione e si dovrebbero sviluppare nuovi strumenti per condurre operazioni comuni e per lo scambio d'informazioni. Un numero crescente di autorità doganali concorda sulla necessità di costituire reti internazionali d'informazione, nel debito rispetto delle disposizioni in materia di protezione dei dati, per agevolare lo scambio d'informazioni. Occorre inoltre investire maggiori risorse in questo settore, sia per migliorare i sistemi informatici, sia per formare il personale, affinché le autorità doganali possano assolvere ai loro compiti in modo più efficace.

## **5.5. Poteri in materia di procedura penale e giurisdizione**

A livello nazionale, una volta soddisfatte le condizioni necessarie stabilite dalla legge, le autorità preposte all'applicazione della legge devono poter ricercare e sequestrare i dati conservati negli elaboratori abbastanza rapidamente da poter evitare la distruzione del materiale probatorio. Le autorità suddette reputano di dover disporre di adeguati poteri di coercizione per condurre, all'interno della loro giurisdizione, ricerche nei sistemi informatici e sequestrare dati, ingiungere la consegna di dati informatici specifici, ordinare od ottenere la tempestiva conservazione di dati specifici, nel rispetto delle normali misure di salvaguardia giuridica e delle procedure legali. Attualmente, tuttavia, tali misure di salvaguardia e procedure non sono armonizzate.

I problemi sorgono qualora accedendo ad un elaboratore le autorità constatino il coinvolgimento di diversi elaboratori e reti, situati sull'intero territorio del paese. La questione si complica qualora, effettuando ricerche in un elaboratore o semplicemente nell'ambito di un'indagine, le autorità preposte all'applicazione della legge accedano senza intenzione o debbano invece accedere a dati localizzati in un altro paese o in diversi altri paesi. Entrano in gioco importanti questioni di sovranità, diritti dell'uomo e interessi relativi all'applicazione della legge per le quali occorre trovare un'adeguata soluzione.

Gli attuali strumenti giuridici di cooperazione internazionale in materia penale, ossia l'assistenza giudiziaria reciproca, possono rivelarsi inadatti o insufficienti, poiché la loro

---

<sup>56</sup> All'articolo 1, paragrafo 4 della posizione comune si legge: "Gli Stati membri dovrebbero sostenere l'elaborazione di disposizioni che favoriscano la cooperazione internazionale, incluse disposizioni sulla più ampia assistenza giudiziaria reciproca possibile. La convenzione dovrebbe facilitare la cooperazione veloce per quanto attiene ai reati connessi con l'informatica o commessi a mezzo computer. Questa forma di cooperazione potrebbe comprendere la creazione di punti di contatto responsabili per l'applicazione della legge operanti 24 ore al giorno, a complemento delle strutture già esistenti di assistenza giudiziaria."

<sup>57</sup> Reperibile sul sito della rete giudiziaria europea, all'indirizzo: <http://ue.eu.int/ejn/index.htm>.

applicazione richiede diversi giorni, settimane o mesi. Occorre un meccanismo che consenta agli Stati d'indagare su reati e di ottenere materiale probatorio in modo rapido ed efficiente, o per lo meno che eviti che nel corso delle procedure per l'applicazione della legge vadano perdute importanti prove, ossia un meccanismo coerente con i principi della sovranità nazionale e della costituzionalità e con i diritti umani, compresa la tutela della sfera privata e la protezione dei dati.

Tra le nuove proposte esaminate nel quadro del progetto di Convenzione sulla criminalità telematica del Consiglio d'Europa che trattano questi problemi, vi sono gli ordini di conservare i dati per coadiuvare indagini specifiche. Altre questioni tuttavia, quali la ricerca ed il sequestro transfrontalieri sollevano spinosi problemi di linea di condotta, non ancora risolti. Occorre palesemente procedere ad un ulteriore scambio dialettico tra le parti interessate, prima di contemplare delle iniziative concrete.

Il sottogruppo che si occupa di criminalità ad alta tecnologia in seno al G8 ha discusso la questione della ricerca e del sequestro transfrontalieri e, anticipando un successivo accordo di carattere più permanente, ha raggiunto un consenso su dei principi provvisori<sup>58</sup>. Restano tuttavia aperte questioni importanti, in particolare circa la possibilità in particolari situazioni di condurre una ricerca ed un sequestro giudiziario rapido, senza informare preliminarmente lo Stato in cui si effettua la ricerca, e si dovranno stabilire delle opportune disposizioni di tutela per garantire il rispetto dei diritti fondamentali. Nella posizione comune adottata sul progetto di convenzione del C.d'E. sulla cibercriminalità i ministri hanno adottato un testo che lascia indefinita la questione.<sup>59</sup>

Nelle azioni penali concernenti reati informatici di portata transnazionale è importante che vi siano disposizioni chiare circa l'attribuzione della competenza per il procedimento penale. Si dovrebbe segnatamente evitare che si creino situazioni in cui nessuno Stato può esercitare la propria giurisdizione. Le principali disposizioni proposte nel progetto di convenzione del Consiglio d'Europa prevedono che la competenza giurisdizionale spetti allo Stato sul cui territorio è commesso il reato o di cui è cittadino l'autore del reato. Qualora più Stati rivendichino la competenza giurisdizionale, questi dovrebbero consultarsi per stabilire la giurisdizione più appropriata. Si tratta di validi principi, ma la consultazione bilaterale o multilaterale ha un peso determinante. La Commissione s'impegna ad esaminare questa problematica per appurare se occorran ulteriori iniziative a livello comunitario.

La Commissione, avendo partecipato alle discussioni in seno sia al C.d'E. che al G8, è consapevole della complessità e delle difficoltà inerenti alle questioni di procedura penale. Un'efficiente cooperazione all'interno dell'UE nella lotta alla criminalità telematica è tuttavia un elemento fondamentale di una società dell'informazione più sicura e per l'instaurazione di un'area di libertà, sicurezza e giustizia.

---

<sup>58</sup> Cfr. il comunicato della Conferenza dei ministri del G8 sulla lotta alla criminalità transfrontaliera organizzata, svoltasi a Mosca il 19 e 20 ottobre 1999 (reperibile al sito <http://www.usdoj.gov/criminal/cybercrime/action.htm> e <http://www.usdoj.gov/criminal/cybercrime/principles.htm>).

<sup>59</sup> GU L 142/2: "Fatti salvi i principi costituzionali e specifiche garanzie intesi ad assicurare l'adeguato rispetto della sovranità, la sicurezza, l'ordine pubblico o altri interessi essenziali di altri Stati, una ricerca informatizzata transfrontaliera ai fini di un'indagine relativa ad un reato penale grave, che verrà ulteriormente definito nella convenzione, può essere presa in considerazione in casi eccezionali, in particolare in presenza di un'emergenza, ad esempio se necessario per impedire la distruzione o l'alterazione di prove di detto reato grave, o per impedire la commissione di un reato che potrebbe causare la morte o un grave pregiudizio all'integrità fisica di una persona."

La Commissione intende proseguire nei prossimi mesi le consultazioni con tutte le parti interessate per portare avanti quest'impegno. Il tema verrà inoltre trattato nel contesto più ampio dell'attività volta alla realizzazione concreta delle conclusioni del Consiglio europeo di Tampere dell'ottobre 1999. In particolare, la conferenza al vertice di Tampere ha invitato il Consiglio e la Commissione ad approvare, entro la fine dell'anno 2000, un programma di misure per l'applicazione del principio del riconoscimento reciproco delle decisioni giudiziarie. La Commissione ha già pubblicato una comunicazione sul riconoscimento reciproco delle decisioni definitive in materia penale<sup>60</sup>. Nell'ambito del proprio contributo al programma di misure in materia di applicazione dei provvedimenti istruttori, la Commissione esaminerà le varie possibilità di riconoscimento reciproco di provvedimenti istruttori in relazione ai reati telematici, nell'ottica di presentare una proposta legislativa nel quadro del Titolo VI del trattato dell'Unione europea.

## **5.6. Valore probatorio dei dati informatici**

Anche nei casi in cui le autorità preposte all'applicazione della legge accedano a dati informatici che sembrano costituire una prova di reato penale, occorre che riescano a reperirli e ad autenticarli, per poterli usare nelle istruttorie e nei procedimenti penali. Non è un'impresa facile, vista la volatilità dei dati elettronici e la facilità con cui possono essere manipolati, falsificati, protetti con dispositivi tecnologici o cancellati. La questione è trattata dall'informatica legale, ramo dei servizi tecnici-scientifici della polizia, che si occupa dello sviluppo e dell'impiego di protocolli e procedure scientifiche per la ricerca negli elaboratori e l'analisi e la salvaguardia dell'autenticità dei dati reperiti.

Su richiesta degli esperti del G8, l'organizzazione internazionale del materiale probatorio informatico (International Organisation of Computer Evidence - IOCE) ha accettato di elaborare raccomandazioni per delle norme, compresa la definizione di termini comuni, l'individuazione dei metodi e delle tecniche da impiegare e la fissazione di un formato comune per le richieste scientifiche-legali. L'Unione dovrebbe partecipare a questi lavori, sia a livello di organismi speciali d'indagine per i reati informatici degli Stati membri sia attraverso l'attività di R&S finanziata nell'ambito del 5° programma quadro (Programma TSI).

## **6. MISURE DI CARATTERE NON LEGISLATIVO**

Occorre un'opportuna normativa a livello sia nazionale che internazionale, ma questo non basta a combattere in modo efficace la criminalità informatica e l'uso illecito delle reti. Occorrono anche delle misure supplementari di carattere non legislativo, per integrare le misure legislative. La maggioranza di queste misure è stata inclusa nelle raccomandazioni dello studio COMCRIME; il G8 ha proposto delle misure nel piano d'azione articolato in 10 punti, che sono state accolte con ampio favore dalle parti nel corso del processo informale di consultazione che ha preceduto la redazione della presente comunicazione. Tra queste figurano:

- l'istituzione a livello nazionale di unità speciali di polizia informatica, nel caso non siano già state create;
- una migliore cooperazione tra gli organi incaricati dell'applicazione della legge, gli operatori del settore, le organizzazioni dei consumatori e i garanti della protezione dei dati;

---

<sup>60</sup> COM (2000) 495, Bruxelles 26.7.2000.

- la promozione di opportune iniziative degli operatori del settore e della collettività, comprese le iniziative riguardanti prodotti di sicurezza.

In questo contesto, la problematica della crittazione continuerà probabilmente ad essere importante. La crittazione è uno strumento fondamentale atto a favorire l'applicazione e il ricorso a nuovi servizi, compreso il commercio elettronico, e a contribuire in modo sostanziale alla prevenzione della criminalità su Internet. La politica della Commissione in materia di crittazione è esposta nella comunicazione del 1997 sulla sicurezza e l'affidabilità nelle comunicazioni elettroniche<sup>61</sup>, nella quale la Commissione ha annunciato che si sarebbe impegnata ad eliminare tutte le restrizioni alla libera circolazione dei prodotti di crittazione nella Comunità europea. In tale documento, la Commissione ha inoltre dichiarato che le limitazioni nazionali alla libera circolazione di tali prodotti devono essere compatibili con il diritto comunitario e che esaminerà se esse siano giustificate e conformi al principio della proporzionalità, segnatamente sulla base delle disposizioni in materia di libera circolazione del trattato, della giurisprudenza della Corte di giustizia e dei requisiti delle direttive sulla protezione dei dati. Nondimeno, la Commissione riconosce che la crittazione è a sua volta fonte di nuove e ardue sfide per gli organismi preposti all'applicazione della legge.

La Commissione si compiace pertanto dell'adozione del testo emendato del regolamento sui beni a duplice uso, che ha contribuito in grande misura a rendere liberamente disponibili i prodotti di crittazione, ma riconosce al medesimo tempo la necessità che questo processo sia accompagnato da un migliore dialogo tra gli utilizzatori, gli operatori e le autorità cui compete l'applicazione della legge. Dal canto suo, la Commissione intende promuovere questo dialogo a livello comunitario, attraverso il prospettato Forum dell'UE. La disponibilità in tutta l'Unione europea di prodotti di sicurezza - compresi dei potenti programmi di crittazione -, certificati se del caso in base a criteri di valutazione concordati, migliorerebbe le possibilità sia di prevenire la criminalità che di accrescere la fiducia degli utenti nei processi della società dell'informazione.

### **6.1. Unità speciali a livello nazionale**

Vista la complessità tecnica e giuridica di alcuni reati informatici, è assolutamente indispensabile che si istituiscano unità speciali a livello nazionale. Tali unità, formate da addetti istruiti e con una preparazione multidisciplinare (nelle attività di applicazione della legge e nelle indagini giudiziarie) dovrebbero essere dotate di adeguate strutture tecniche ed operare come punti di contatto con il compito di:

- rispondere prontamente alle richieste d'informazione relative a presunti reati. I formati comuni per lo scambio di tali informazioni restano ancora da definire, sebbene in sede di discussioni tra esperti in seno al G8 è emerso che non sarà un'impresa facile, a causa delle differenze tra le culture nazionali in campo giuridico;
- fungere da interfaccia per l'applicazione della legge a livello nazionale ed internazionale per le 'linee rosse' ('hotlines')<sup>62</sup> cui confluiscono le denunce di contenuti illeciti trasmesse dagli utilizzatori di Internet;

---

<sup>61</sup> COM (97) 503.

<sup>62</sup> Finora le hotlines (linee dirette d'emergenza) esistono solo in un numero limitato di paesi. Esempi sono rappresentati da Cybertipline negli USA e Internet Watch Foundation (IWF) nel Regno Unito, che da dicembre del 1996, ha attivato una linea telefonica e una casella postale elettronica cui il pubblico può accedere per riferire in merito a materiale incontrato su Internet, ritenuto illecito. La IWF giudica se il materiale è illecito, informa gli ISP e la polizia. Altri organismi di sorveglianza esistono anche in

- migliorare e/o sviluppare speciali tecniche d'indagine informatica per individuare, indagare e avviare procedimenti penali in relazione a reati informatici;
- fungere da centro di eccellenza in materia di reati telematici, per la condivisione delle migliori pratiche e delle esperienze.

Nell'ambito della Comunità, alcuni Stati membri hanno già istituito tali unità speciali, che si occupano specificamente di reati informatici. La Commissione reputa che la loro istituzione sia una prerogativa degli Stati membri ed incoraggia caldamente gli Stati membri stessi a provvedere in tal senso. L'acquisto delle apparecchiature più moderne e dei programmi informatici più recenti, nonché la formazione del personale addetto comportano ingenti costi e presuppongono la formulazione di priorità e l'adozione di decisioni politiche ai vari livelli dello Stato.<sup>63</sup> L'esperienza maturata nelle unità già esistenti può essere particolarmente preziosa. La Commissione intende incoraggiare lo scambio di tali esperienze.

La Commissione è inoltre convinta che Europol possa apportare un ulteriore prezioso contributo a livello comunitario, attraverso il coordinamento, l'analisi e altre forme di assistenza alle unità speciali nazionali. La Commissione intende pertanto estendere la missione di Europol per includervi la criminalità telematica.

## **6.2. Formazione specializzata**

Occorrono notevoli sforzi sul piano della formazione continua e specializzata sia delle forze di polizia sia del personale giudiziario. Le tecniche e le capacità criminali informatiche evolvono più rapidamente che nei tradizionali settori dell'attività criminosa.

Alcuni Stati membri da tempo conducono iniziative di formazione alle tecnologie avanzate del personale addetto all'applicazione della legge e potrebbero dare consigli e assistenza agli Stati membri che non hanno ancora preso tali misure.

Con il sostegno dei programmi gestiti dalla Commissione (in particolare i programmi STOP, FALCONE e GROTIUS) sono stati avviati dei progetti aventi questa finalità ed impostati come scambio d'esperienze, seminari sulle problematiche comuni che le categorie professionali interessate si trovano ad affrontare. La Commissione proporrà maggiori attività in questo campo e tra queste la formazione informatica e la formazione in rete.

Europol ha preso l'iniziativa di ospitare un convegno di formazione della durata di una settimana rivolto ad addetti di organismi preposti all'applicazione della legge degli Stati membri a novembre del 2000, che darà particolare risalto alle questioni della pornografia infantile. L'ambito di tale convegno potrebbe essere ampliato onde includere la criminalità informatica in generale. Interpol è anch'esso attivo in questo campo da diversi anni. Le sue

---

Norvegia (Redd Barna), nei Paesi Bassi (Meldpunt), in Germania (Newswatch, FSM e Jugendschutz), Austria (ISPAA) ed Irlanda (ISPAI). Nel quadro del programma comunitario Daphne, Childnet International ha attualmente avviato un progetto direttamente connesso a questa problematica ("International Hotline Providers in Europe Forum"). In occasione del convegno di esperti patrocinato dall'UNESCO, svoltosi a Parigi a gennaio del 1999, sono stati espressi adesione e incoraggiamento anche per le linee rosse (hotlines) nazionali e l'istituzione di reti di dette linee o di una "torre di guardia elettronica" internazionale.

<sup>63</sup> Per esperienze in materia negli USA si rinvia a Michael A. Sussmann "The Critical Challenges from International High-Tech and Computer-Related Crime at the Millennium", *Duke Journal of Comparative and International Law*, Vol. 9, primavera 1999, pag. 464.

iniziative in materia potrebbero essere allargate, rendendo la formazione accessibile ad un più elevato numero di partecipanti.

Il G8 ha lanciato delle iniziative volte allo scambio di esperienze tra le autorità preposte all'applicazione della legge e alla fissazione di tecniche comuni d'indagine sulla base di azioni concrete. Un'ulteriore iniziativa nel campo della formazione è prevista per il secondo semestre del 2000 o all'inizio dell'anno 2001. Gli Stati membri che partecipano ai lavori del G8 potrebbero mettere le loro esperienze a disposizione degli altri Stati membri.

Nel campo specifico della lotta alla pornografia infantile su Internet, la creazione e la gestione a livello internazionale di una libreria digitale centrale di immagini pornografiche di minori (accessibile alle varie unità speciali nazionali incaricate dell'applicazione della legge attraverso Internet ed allestita nel rispetto delle debite condizioni e vincoli di accesso e di tutela della riservatezza) aiuterebbe a ricercare le vittime e gli autori dei reati, ad accertare la natura dei reati ed a formare funzionari di polizia specializzati.<sup>64</sup>

### **6.3. Migliori informazioni e regole comuni per la registrazione dei dati**

La fissazione di regole armonizzate per la registrazione dei dati da parte della polizia e delle autorità giudiziarie, nonché la concezione di adeguati strumenti di analisi statistica dei reati informatici aiuterebbero le autorità preposte all'applicazione della legge e le autorità giudiziarie a meglio registrare, analizzare e valutare le informazioni formali raccolte in questo settore in continua evoluzione.

Inoltre, secondo il settore privato, tali dati statistici sono necessari per una giusta valutazione dei rischi, per un'analisi dei costi/benefici connessi alla loro gestione. Questo è importante non solo ai fini operativi (quale la scelta delle misure di sicurezza da adottare), ma anche a fini assicurativi.

Si sta attualmente aggiornando e rendendo accessibile alla Commissione una base dati sulle normative in materia di criminalità informatica, allestita nell'ambito dello studio COMCRIME. La Commissione esaminerà la possibilità di migliorarne il contenuto (per includervi leggi, giurisprudenza e bibliografia) e l'usabilità.

---

<sup>64</sup> In questo contesto il progetto "Excalibur" sviluppato dal dipartimento nazionale svedese d'informazione sulla criminalità (Swedish National Crime Intelligence Division) e cofinanziato dalla Commissione europea nell'ambito del programma STOP si è rivelato un successo. Tale progetto è stato allestito con la cooperazione delle forze di polizia della Germania, del Regno Unito, dei Paesi Bassi e del Belgio, assieme a Europol e Interpol. Altri progetti condotti dalla tedesca BKA (la cosiddetta "Perkeo") e dal Ministero francese dell'interno (progetto "Surfimage" cofinanziato a sua volta nel quadro del programma STOP) devono anch'essi presi in considerazione.

#### 6.4. Cooperazione tra i vari soggetti: il Forum dell'UE

La costruttiva cooperazione tra le autorità statali e gli operatori del settore nell'ambito giuridico è considerata un elemento fondamentale di qualsiasi politica pubblica volta a debellare i reati informatici.<sup>65</sup> I rappresentanti degli organismi preposti all'applicazione della legge hanno ammesso di non aver sempre espresso con chiarezza e precisione che cosa si aspettino dai prestatori di servizi. I rappresentanti degli operatori del settore hanno manifestato una generale disponibilità verso una migliore cooperazione con le autorità preposte all'applicazione della legge, sottolineando al contempo la necessità di conciliare la tutela dei diritti fondamentali e delle libertà dei cittadini, segnatamente il diritto alla riservatezza,<sup>66</sup> con la lotta contro la criminalità e gli oneri economici gravanti sui prestatori.

Assieme, gli operatori e le autorità preposte all'applicazione della legge possono sensibilizzare i cittadini ai rischi derivanti dall'operato dei criminali su Internet, promuovere le migliori pratiche per la sicurezza, nonché sviluppare efficaci strumenti e procedure per contrastare la criminalità. In diversi Stati membri sono già state lanciate iniziative in questo campo; tra queste si annovera l'Internet Crime Forum, istituito nel Regno Unito, probabilmente l'iniziativa di più vecchia data e di più ampia portata.<sup>67</sup>

La Commissione plaude a queste iniziative e ritiene che debbano essere incoraggiate in tutti gli Stati membri. La Commissione intende istituire un Forum dell'UE, cui aderirebbero gli organismi incaricati dell'applicazione della legge, i prestatori di servizi Internet (ISP), i gestori di telecomunicazioni, le organizzazioni per la tutela dei diritti civili, i rappresentanti dei consumatori e le autorità garanti della protezione dei dati, nonché le altre parti interessate, con l'obiettivo di rafforzare la cooperazione a livello comunitario. In una prima fase, ai lavori parteciperebbero i funzionari pubblici designati dagli Stati membri, esperti in tecnologie, esperti in materia di riservatezza, designati dal Gruppo per la tutela delle persone con riguardo al trattamento dei dati personali, istituito a norma dell'articolo 29, nonché i rappresentanti degli operatori del settore e dei consumatori, prescelti in base a dirette consultazioni con gli operatori del settore e le associazioni di consumatori. In una seconda fase, alle attività del Forum parteciperebbero i rappresentanti delle varie iniziative nazionali.

Il Forum dell'UE sarà gestito in modo aperto e trasparente, i relativi documenti saranno pubblicati su un sito Internet e tutte le parti interessate saranno invitate a trasmettere le loro osservazioni.

---

<sup>65</sup> Nel comunicato emanato a Washington il 9/10 dicembre 1997 sui principi e il piano d'azione articolato in 10 punti per la lotta contro la criminalità ad alta tecnologia, approvato dai ministri della giustizia e degli affari interni del G8, si afferma: "Il settore industriale concepisce, installa e provvede al funzionamento di queste reti globali e ad esso compete sostanzialmente lo sviluppo di norme tecniche. Spetta pertanto agli operatori del settore contribuire allo sviluppo e alla distribuzione di sistemi sicuri, concepiti per captare l'uso abusivo di mezzi informatici, conservare il materiale probatorio elettronico e coadiuvare le autorità nell'accertamento della localizzazione e dell'identità degli autori di reati penali". La decisione del Consiglio UE di lottare contro la pornografia infantile su Internet sottolinea la necessità che gli Stati membri intavolino un dialogo costruttivo con gli operatori del settore e che, in contatto con essi, cooperino ad uno scambio di esperienze.

<sup>66</sup> Come stabilito nelle direttive comunitarie sulla protezione dei dati, nella convenzione del Consiglio d'Europa sui diritti dell'uomo e nella convenzione n. 108 del Consiglio d'Europa per la tutela delle persone fisiche con riguardo al trattamento automatico dei dati personali e il diritto nazionale in materia.

<sup>67</sup> All'Internet Crime Forum - istituito nel 1997 - aderiscono agenti di polizia, funzionari del ministero degli interni e rappresentanti di operatori di Internet; indice riunioni plenarie 3-4 volte all'anno e conta diversi gruppi di lavoro permanenti.

Il Forum dell'UE sarà invitato ad occuparsi in particolare di quanto segue:

- sviluppare, eventualmente, punti di contatto, attivi 24 al giorno, tra gli organi statali e gli operatori del settore;
- sviluppare un valido formato uniforme per le richieste d'informazione delle autorità preposte all'applicazione della legge, agli operatori del settore, diffondendo l'uso di Internet da parte delle suddette autorità nelle comunicazioni con i prestatori di servizi;
- incoraggiare lo sviluppo e/o l'applicazione di codici di condotta e delle migliori pratiche, nonché la loro adozione da parte degli operatori e delle autorità<sup>68</sup>;
- incoraggiare lo scambio d'informazioni sulle tendenze della criminalità ad alta tecnologia tra le varie parti, in particolare tra operatori ed autorità preposte all'applicazione della legge;
- esaminare le eventuali problematiche dell'applicazione della legge nell'ambito dello sviluppo delle nuove tecnologie;
- incoraggiare l'ulteriore sviluppo di meccanismi di preallarme e di gestione di crisi per prevenire, individuare e affrontare minacce o avvenimenti suscettibili di compromettere il funzionamento delle infrastrutture dell'informazione;
- fornire, ove necessario, un maggiore contributo specialistico alle attività condotte in seno al Consiglio e ad altri consessi internazionali, quale ad esempio il Consiglio d'Europa e il G8;
- incoraggiare la cooperazione tra le parti interessate, per giungere tra l'altro a principi comuni, condivisi dalle autorità preposte all'applicazione della legge, dagli operatori del settore e dagli utilizzatori (ad es. elaborazione di un documento d'intesa (Memorandum of Understanding - MOU), codici di prassi conformi al contesto giuridico stabilito).

## **6.5. Azioni dirette degli operatori del settore**

La lotta alla criminalità informatica è in grande misura nell'interesse della società in senso lato. Se si vuole che i consumatori abbiano fiducia nel commercio elettronico, le misure di prevenzione della criminalità informatica dovranno diventare un elemento scontato di buona pratica commerciale. Molti settori, ad es. quello bancario, delle comunicazioni elettroniche, delle carte di credito e dei diritti d'autore e i loro clienti sono potenziali vittime della criminalità informatica. Le imprese tutelano naturalmente i loro nomi e marchi e svolgono pertanto una funzione nella prevenzione delle frodi. Le organizzazioni che rappresentano i settori del software e dei prodotti audio (ad es. la British Phonographic Industry - BPI) dispongono di squadre apposite, che indagano su eventuali piraterie (compresa la pirateria commessa via Internet). In diversi Stati membri i fornitori di servizi Internet hanno istituito delle linee speciali (hotlines) per la denuncia di informazioni di contenuto illegale e nocivo.

---

<sup>68</sup> I codici di condotta ai sensi dell'articolo della direttiva 95/46/CE (che potrebbero riguardare questioni disciplinate dalla direttiva 97/66/CE, quale la crittazione) sono discussi dal Gruppo per la tutela delle persone in riguardo al trattamento dei dati personali, istituito a norma dell'articolo 29, e le autorità di controllo competenti in materia di protezione dei dati.

La Commissione ha sostenuto alcune di queste iniziative, incoraggiandone l'inclusione nel programma quadro di R&S della Comunità, nel piano d'azione per Internet<sup>69</sup> nonché nei programmi condotti nell'ambito del Titolo VI, quali STOP e DAPHNE.

Nell'ambito del Forum dell'UE si scambierà la migliore pratica in questi settori.

## **6.6. Progetti di RST finanziati dall'UE**

Nel programma di RST relativo alla società dell'informazione (TSI), che rientra nel 5° programma quadro, per il periodo 1998 - 2002, l'accento è posto sullo sviluppo e l'applicazione di tecnologie atte a creare la fiducia. Tra le tecnologie aventi tale finalità rientrano sia le tecnologie per la sicurezza dell'informazione e delle reti, sia gli strumenti e le procedure tecniche di salvaguardia dalle violazioni del diritto fondamentale alla riservatezza e alla protezione dei dati, nonché di altri diritti della persona e per combattere la criminalità informatica.

Il programma TSI, ed in particolare l'attività connessa alla *sicurezza delle informazioni e delle reti e altre tecnologie volte a creare fiducia* nell'ambito dell'azione chiave 2, intitolata *Nuovi metodi di lavoro e commercio elettronico*, offre il quadro per lo sviluppo di capacità e tecnologie per comprendere e far fronte alle sfide tecnologiche che si vanno profilando nella prevenzione e lotta alla criminalità informatica, e garantire il soddisfacimento di requisiti di sicurezza e riservatezza a livello comunitario, a livello delle comunità virtuali e a livello del cittadino.

Inoltre, nel contesto del programma TSI è stata avviata anche un'iniziativa riguardante l'affidabilità, per poter affrontare in modo adeguato le sfide connesse alla fiducia e alla percezione di sicurezza, compresa la prevenzione e l'attività investigativa sulla criminalità informatica. Questa iniziativa deve contribuire ad accrescere e a diffondere la fiducia nei confronti delle infrastrutture d'informazione caratterizzate da un elevato grado di interoperabilità e nei sistemi incorporati in rete, propagando la percezione di affidabilità e le tecnologie che permettono di realizzare tale affidabilità. Un elemento integrale di quest'iniziativa è la cooperazione internazionale. Nell'ambito del programma TSI si sono sviluppati dei rapporti di lavoro con DARPA e NSF ed è stata istituita, in collaborazione con il Dipartimento di Stato, una Task Force comune per la protezione dell'infrastruttura critica, sotto l'egida del gruppo consultivo paritetico CE/USA istituito nell'ambito dell'accordo di cooperazione S&T.<sup>70</sup>

Il Centro comune di ricerca (CCR), che ha cooperato all'iniziativa sull'affidabilità condotta nell'ambito del programma TSI, concentrerà i propri sforzi sullo sviluppo di opportune misure armonizzate, di indicatori e dati statistici, consultando le altre parti interessate, compreso Europol. Tale attività sarà finalizzata all'elaborazione di un'adeguata classificazione delle attività illecite e alla loro comprensione, distribuzione geografica, alla determinazione del loro tasso d'incremento e dell'efficacia delle misure adottate per contrastarle. Laddove opportuno, il CCR coinvolgerà altri gruppi di ricerca e integrerà i loro sforzi e i risultati dei loro lavori. Esso s'incarica inoltre di gestire un sito Internet sull'argomento e di riferire al Forum dell'UE in merito alla sua evoluzione.

---

<sup>69</sup> Per maggiori ragguagli sul piano d'azione per Internet: Il piano d'azione volto a promuovere l'uso più sicuro di Internet è reperibile all'indirizzo <http://158.169.50.95:10080/iap/>.

<sup>70</sup> Maggiori ragguagli circa il programma TSI sono reperibili al sito <http://www.cordis.lu/ist>.

## 7. CONCLUSIONI E PROPOSTE

La prevenzione e la lotta efficace contro la criminalità informatica esigono il soddisfacimento di determinate condizioni:

- la disponibilità di tecnologie per la prevenzione. Ciò richiede un adeguato contesto normativo, che lasci spazio e incentivi all'innovazione e alla ricerca. L'intervento finanziario pubblico può essere necessario per sostenere lo sviluppo e l'applicazione di adeguate tecnologie per la sicurezza;
- la conoscenza dei potenziali rischi sul piano della sicurezza e dei metodi per combatterli;
- disposizioni di diritto penale sostanziali e procedurali adeguate, nei confronti delle attività criminose sia transnazionali che nazionali. Le disposizioni sostanziali di diritto penale dei vari Stati dovrebbero essere sufficientemente complete ed efficaci per poter perseguire penalmente i gravi illeciti informatici e comminare sanzioni dissuasive, contribuendo a superare i problemi della duplice requisito di perseguibilità del reato<sup>71</sup> ed agevolare la cooperazione internazionale. Qualora le autorità preposte all'applicazione della legge abbiano la fondata necessità di agire tempestivamente e ricercare, reperire e assicurarsi una copia di dati informatici nell'ambito del territorio nazionale, per poter indagare su un reato informatico, il diritto processuale dovrebbe consentire tale azione in conformità con i principi e le deroghe stabilite dal diritto comunitario e in conformità alla Convenzione europea sui diritti dell'uomo. La Commissione è convinta che l'accordo raggiunto sulle disposizioni in materia di intercettazioni, nell'ambito della Convenzione sull'assistenza giudiziaria in materia penale costituisca il traguardo massimo attuale. La Commissione continuerà a verificarne l'applicazione assieme agli Stati membri, agli operatori del settore e agli utilizzatori, per garantire l'efficacia, la trasparenza e l'equilibrio delle iniziative in questione;
- la disponibilità di un sufficiente numero di addetti per l'applicazione della legge ben preparati ed attrezzati. Si incoraggerà ulteriormente la stretta collaborazione nel campo della formazione con i fornitori di servizi Internet ed i gestori di telecomunicazioni;
- una migliore cooperazione tra tutti i soggetti in causa: utilizzatori e consumatori, operatori del settore, autorità preposte all'applicazione della legge e autorità di controllo competenti in materia di protezione dei dati. Questo requisito è critico per le indagini sulla criminalità informatica e per la tutela della sicurezza pubblica. Occorre che gli operatori del settore agiscano nel rispetto di chiare regole ed obblighi. I governi dovrebbero rendersi conto che le esigenze dell'applicazione della legge impongono degli oneri agli operatori del settore e dovrebbero pertanto adottare provvedimenti ragionevoli per minimizzare tali oneri. Al tempo stesso, gli operatori del settore dovrebbero tener conto della sicurezza pubblica nelle loro pratiche commerciali. Questo richiederà una crescente cooperazione attiva ed il sostegno da parte del singolo utilizzatore e consumatore;

---

<sup>71</sup> Nei casi in cui le istruttorie penali richiedano l'assistenza di autorità giudiziarie di un altro paese, molti ordinamenti giuridici esigono che la fattispecie configuri un reato in entrambi i paesi: si tratta di un requisito necessario per determinati tipi di assistenza giudiziaria reciproca e per l'estradizione.

- continue iniziative da parte degli operatori del settore e della comunità degli utenti. Le linee rosse (hotlines), già esistenti per la denuncia di casi di informazioni di contenuto illegale e nocivo potrebbero essere estese per altri tipi di abuso. All'iniziativa di autoregolamentazione degli operatori del settore e all'elaborazione di un documento d'intesa di portata multidisciplinare, potrebbe partecipare il massimo numero di parti interessate, che svolgerebbero molteplici funzioni, nella prevenzione e nella lotta contro la criminalità informatica nonché per la sensibilizzazione e la propagazione della fiducia;
- i risultati e le potenzialità offerte dalla R&S dovrebbero essere sfruttati al massimo. La strategia sarà essenzialmente tesa alla convergenza tra la sicurezza ad un prezzo accessibile ed efficace e altri sviluppi tecnologici, volti a diffondere la fiducia, nonché le iniziative strategiche comunitarie.

Tutte le eventuali misure da concordare con la Comunità dovrebbero tuttavia tenere conto della necessità di un graduale inserimento dei paesi candidati all'adesione negli ambiti della cooperazione comunitaria ed internazionale in questo campo e di evitare che i suddetti paesi fungano da paradisi della criminalità informatica. Si dovrebbe valutare la possibilità di coinvolgere dei rappresentanti di questi paesi in alcune o in tutte le riunioni comunitarie in materia.

Le proposte della Commissione possono essere articolate come segue.

### **7.1. Proposte legislative**

La Commissione presenterà delle proposte legislative sulla base del titolo VI del trattato dell'UE volte a:

- ravvicinare ulteriormente le normative penali degli Stati membri in relazione ai reati connessi alla pornografia infantile. Questa iniziativa farà parte di un pacchetto di proposte che riguarderanno anche questioni più generali legate allo sfruttamento sessuale dei minori e alla tratta degli esseri umani, in conformità a quanto annunciato nella comunicazione della Commissione sulla tratta degli esseri umani, del dicembre 1998. Tale proposta sarà conforme all'impegno del Parlamento europeo di convertire l'iniziativa austriaca volta all'emanazione di una decisione del Consiglio sulla pornografia infantile in una decisione quadro, che imponga il ravvicinamento delle leggi. Ciò è inoltre coerente con le conclusioni di Tampere e il documento intitolato 'prevenzione e controllo della criminalità organizzata - strategia dell'Unione europea per l'inizio del nuovo millennio'. La proposta è già stata inserita nel quadro dei risultati per l'instaurazione di uno spazio di libertà, di sicurezza e di giustizia;
- ravvicinare ulteriormente il diritto penale in materia di criminalità ad alta tecnologia. Verranno inseriti i reati connessi all'accesso abusivo ad un sistema informatico o telematico ('hacking'), gli attacchi finalizzati all'interruzione dei servizi. La Commissione esaminerà inoltre le possibilità d'azione per combattere il razzismo e la xenofobia su Internet, nell'ottica di presentare una decisione quadro nell'ambito del Titolo VI del trattato dell'Unione europea, concernente le attività razzistiche e xenofobiche in rete e non. Da ultimo si esaminerà il problema del commercio di sostanze stupefacenti illecite tramite Internet;

- applicare il principio del riconoscimento reciproco dei provvedimenti istruttori connessi a reati telematici, nonché agevolare le indagini penali relative ai reati informatici che coinvolgano più di uno Stato membro, applicando debite disposizioni di tutela dei diritti fondamentali. Questa proposta è coerente con il programma relativo alle misure per il reciproco riconoscimento, in cui si menziona la necessità di esaminare proposte in materia di reperimento e sequestro del materiale probatorio.

La necessità di adottare eventuali misure, particolare di carattere legislativo, relative alla conservazione di dati sul traffico verranno valutate dalla Commissione, nell'ambito di altre consultazioni, alla luce dei risultati dei lavori svolti dal Forum dell'UE di cui si è prospettata la costituzione.

## **7.2. Proposte di carattere non legislativo**

Si propone l'azione in alcune aree.

- La Commissione istituirà e presiederà un Forum dell'UE, cui aderiranno gli organismi preposti all'applicazione della legge, i prestatori di servizi, i gestori di reti, i gruppi di consumatori e i garanti della protezione dei dati, con lo scopo di rafforzare la cooperazione a livello comunitario mediante: la sensibilizzazione del pubblico ai rischi connessi all'attività criminale su Internet; la promozione delle migliori pratiche per la sicurezza IT; lo sviluppo di efficaci strumenti e procedure per contrastare la criminalità informatica; la promozione dell'ulteriore sviluppo di meccanismi di preallarme e di gestione di crisi. Si tratterebbe di una versione comunitaria di fori analoghi esistenti in taluni Stati membri. La Commissione intende incoraggiare gli Stati membri ad istituirli, laddove non esistono. Il Forum dell'UE incoraggerà ed agevolerà la cooperazione tra questi diversi fori.
- La Commissione continuerà a promuovere la sicurezza e la fiducia nel contesto dell'iniziativa *eEurope*, del piano d'azione per Internet, del programma TSI e del prossimo programma quadro per la RTS. In questi contesti, si promuoverà la disponibilità di prodotti e servizi aventi un adeguato livello di sicurezza e si incoraggerà un uso più liberalizzato di potenti sistemi di crittazione, attraverso il dialogo tra tutte le parti interessate.
- La Commissione promuoverà ulteriori progetti nel quadro degli attuali programmi a favore della formazione del personale degli organismi preposti all'applicazione della legge in materia di criminalità ad alta tecnologia e a favore della ricerca nel settore dell'informatica legale.
- La Commissione vaglierà la possibilità di stanziare fondi per migliorare il contenuto e l'utilizzabilità della base dati sulle normative nazionali degli Stati membri, costituita nell'ambito dello studio COMCRIME, e condurrà uno studio volto a tracciare un quadro più preciso della tipologia e della portata della criminalità informatica negli Stati membri.

## **7.3. Iniziative in altre sedi internazionali**

La Commissione continuerà a svolgere appieno la propria funzione di coordinamento tra gli Stati membri in altre sedi internazionali che trattano la criminalità telematica, quali il Consiglio d'Europa e il G8. Le iniziative della Commissione a livello comunitario terranno pienamente conto dei progressi compiuti nell'ambito di altre istanze internazionali, pur continuando l'opera di ravvicinamento delle normative nazionali all'interno dell'Unione europea.

\* \* \* \*

## SCHEDA FINANZIARIA

### **1. DENOMINAZIONE DELL'AZIONE**

Creare una società dell'informazione sicura migliorando la sicurezza delle infrastrutture dell'informazione e mediante la lotta alla criminalità informatica.

### **2. VOCI DI BILANCIO**

B5 302

B5 820

B6 1110, B6 2111, B6 1210

### **3. BASE GIURIDICA**

Artt. 95, 154 e 155 del trattato CE e artt. 29 e 34 del trattato UE.

### **4. DESCRIZIONE DELL'AZIONE**

#### **4.1. Obiettivo generale**

La Commissione istituirà e presiederà un Forum dell'UE, cui aderiranno gli organismi preposti all'applicazione della legge, i prestatori di servizi Internet (ISP), i gestori di telecomunicazioni, le organizzazioni per la tutela dei diritti civili, i rappresentanti dei consumatori, i garanti della protezione dei dati e le altre parti interessate, con lo scopo di promuovere la comprensione e la cooperazione a livello dell'Unione europea. Il Forum si adopererà per sensibilizzare il pubblico ai rischi connessi all'attività criminale su Internet, promuovere le migliori pratiche per la sicurezza IT, individuare efficaci strumenti e procedure atti a contrastare la criminalità informatica, nonché per promuovere l'ulteriore sviluppo di meccanismi di preallarme e di gestione di crisi. I documenti pertinenti saranno pubblicati sul sito Internet.

#### **4.2. Durata e modalità di rinnovo**

2001 – 2002. Nel 2002, si valuterà se mantenere il Forum.

### **5. CLASSIFICAZIONE DELLE SPESE/ENTRATE**

#### **5.1. Spese non obbligatorie**

#### **5.2. Stanziamenti dissociati**

## 6. NATURA DELLE SPESE/ENTRATE

<b>Riunioni: spese di viaggio rimborso esperti</b>			
B5 302A	2001		27.000 €
B5 302A	2002		40.500 €
<b>Attività del Forum, gestione di un sito Internet</b>			
B6 1110	2001	Missioni CCR	10.000 €
B6 2111	2001	Dotazioni specifiche (varie) CCR	15.000 €
B6 1210	2001	Fondi spese indirette CCR	50.000 €
B6 1110	2002	Missioni CCR	10.300 €
B6 2111	2002	Dotazioni specifiche (varie) CCR	15.450 €
B6 1210	2002	Fondi spese indirette CCR	51.500 €
<b>Studi su temi specifici</b>			
B6 2111	2001	Dotazioni specifiche (studi) CCR	25.000 €
B6 2111	2002	Dotazioni specifiche (studi) CCR	25.750 €
Totale	2001 + 2002		270.500 €

## 7. INCIDENZA FINANZIARIA

**Metodo di calcolo del costo totale dell'azione (relazione tra costi singoli e costi complessivi):**

Rimborso spese di viaggio dei partecipanti alle riunioni. Si calcola che nel 2001 e nel 2002 si terranno rispettivamente 2 e 3 riunioni. Per ogni riunione si prevede di rimborsare le spese di 15 esperti. Il costo medio procapite del rimborso è stimato a 900 €.

I costi, riferiti sia al personale che a dotazioni specifiche, dell'infrastruttura e di sostegno amministrativo e tecnico sono imputati in funzione del numero di addetti assegnati alle attività in questione. La dotazione finanziaria relativa agli studi è calcolata sulla base di 2 studi all'anno, pari ad 1 persona/mese ciascuno.

## 8. DISPOSIZIONI ANTIFRODE

Controlli ordinari. Non sono contemplate misure supplementari di prevenzione delle frodi.

## 9. ELEMENTI DELL'ANALISI COSTO-EFFICACIA

### 9.1. Obiettivi specificati e quantificabili; beneficiari

Migliorare la comprensione e la cooperazione tra i diversi gruppi d'interesse a livello dell'Unione. Partecipanti selezionati: organismi preposti all'applicazione della legge, prestatori di servizi Internet (ISP), gestori di telecomunicazioni, organizzazioni per la tutela dei diritti civili, rappresentanti dei consumatori, garanti della protezione dei dati e altre parti interessate.

### 9.2. Giustificazione dell'azione

Il Forum è istituito allo scopo di migliorare la comprensione e la cooperazione tra i diversi gruppi d'interesse a livello dell'Unione. Il Forum si adopererà per sensibilizzare il pubblico ai rischi connessi all'attività criminale su Internet, promuovere le migliori pratiche per la sicurezza IT, individuare efficaci strumenti e procedure atti a contrastare la criminalità informatica e promuovere l'ulteriore sviluppo di meccanismi di preallarme e di gestione di crisi.

### 9.3. Controllo e valutazione dell'azione

La Commissione organizzerà e presiederà le riunioni del Forum e parteciperà alle discussioni. La Commissione gestirà il sito web corrispondente. Nel 2002 si valuterà se il Forum debba continuare la propria attività nel 2003 e oltre.

## 10. SPESE AMMINISTRATIVE

Le esigenze in termini di risorse umane saranno soddisfatte nell'ambito dell'attuale organico.

### 10.1. Incidenza sul numero di posti

Tipo di posto	Personale da assegnare alla gestione dell'attività		Fonte		Durata
	Posti permanenti	Posti temporanei	Risorse disponibili nelle DG	Risorse supplementari	
Funzionari o temporanei					all'anno per 2 due anni
A		1,75	1,75		
B		0,15	0,15		
C	0,05		0,05		
Altre risorse					
Totale	0,05	1,9	1,95		

### 10.2 Incidenza finanziaria complessiva delle risorse umane

	Importi	Metodo di calcolo (2001 - 2002)
Funzionari	421.200 €	2 anni x 108.000 € x 1,95 addetti