5.8 Secondo il Comitato il regolamento 4056/86 dovrebbe essere abrogato e sostituito da un nuovo regolamento della Commissione che preveda una nuova esenzione per categoria. Il nuovo sistema dovrebbe seguire rigorosamente i criteri stabiliti dalla giurisprudenza del Tribunale europeo di primo grado e della Commissione (ad esempio la causa TACA). Il sistema delle conferenze dovrebbe essere mantenuto anche per difendere la competitività degli armatori comunitari nel mondo. Mentre per le grandi «alleanze» di vettori e altri tipi di cooperazione gli accordi possono essere adatti, i vettori di piccole e medie dimensioni hanno ancora bisogno di conferenze per mantenere le loro quote di mercato specie nel commercio con i paesi in via di sviluppo. L'abolizione dell'esenzione può avere effetti anticoncorrenziali per questi piccoli vettori, rafforzando la posizione dominante di quelli di maggiori dimensioni.

5.9 Tale periodo transitorio e provvisorio dovrebbe essere impiegato dalla Commissione per monitorare gli sviluppi del mercato dei traffici di linea, comprese le tendenze al consolidamento. Inoltre, la Commissione dovrebbe avviare delle consultazioni con altre organizzazioni (OCSE) per giungere all'adozione di un adeguato sistema alternativo compatibile a livello mondiale.

5.10 Il Comitato appoggia le proposte del Libro bianco relative al trattamento dei servizi non di linea e di cabotaggio, poiché la grande maggioranza dei casi in questi settori non solleverebbe problemi di concorrenza. Tuttavia, in nome della certezza giuridica, chiede alla Commissione di fornire un orientamento giuridico per quanto riguarda l'autovalutazione da parte dei *bulk pool* e delle attività specializzate per quanto concerne la compatibilità con l'articolo 81 del Trattato CE.

5.11 Il Comitato si augura di poter prestare la propria assistenza nelle fasi che seguiranno l'azione di consultazione avviata dal Libro bianco.

Bruxelles, 16 dicembre 2004.

La Presidente
del Comitato economico e sociale europeo
Anne-Marie SIGMUND

Parere del comitato economico e sociale europeo in merito alla proposta di decisione del parlamento europeo e del consiglio che istituisce un programma comunitario pluriennale inteso a promuovere un uso più sicuro di internet e delle nuove tecnologie on-line

COM(2004) 91 def. — 2004/0023 COD

(2005/C 157/24)

Il Consiglio, in data 26 marzo 2004, ha deciso, conformemente al disposto dell'articolo 153 del Trattato che istituisce la Comunità europea, di consultare il Comitato economico e sociale in merito alla proposta di cui sopra.

La sezione specializzata Trasporti, energia, infrastrutture, società dell'informazione, incaricata di preparare i lavori del Comitato in materia, ha formulato il proprio parere in data 5 ottobre 2004, sulla base del progetto predisposto dal relatore RETUREAU e dalla correlatrice DAVISON.

Il Comitato economico e sociale europeo, in data 16 dicembre 2004, nel corso della 413a sessione plenaria, ha adottato il seguente parere con 147 voti favorevoli e 1 astensione.

1. **Sintesi del progetto di parere**

1.1 La Commissione propone di istituire un nuovo programma «Safer Internet», perfezionandolo però in considerazione del rapido evolversi della società dell'informazione con riguardo alle reti di comunicazioni. Il programma è perciò denominato «Safer Internet Plus» (2005-2008).

1.2 Oltre alla proposta di decisione del Parlamento e del Consiglio presentata dalla Commissione, il CESE ha esaminato la relazione di valutazione ex ante di Safer Internet Plus (2005/2008) contenuta in un «Commission staff working paper» SEC (2004) 148 e nel COM(2004) 91 def.. Il Comitato appoggia l'ampliamento del campo di azione del nuovo programma e dei suoi obiettivi al fine di tener conto della rapida evoluzione e della diversificazione dei mezzi di accesso *on-line* nonché della rapidissima crescita del numero degli accessi ad alta velocità e delle connessioni permanenti. Nelle sue osservazioni generali e particolari, esso formula una serie di raccomandazioni complementari circa le azioni politiche e normative, in particolare con riguardo ai seguenti aspetti:

— le norme tecniche e giuridiche (imperative e di autodisciplina),

— l'istruzione-formazione degli utilizzatori,

— gli obblighi dei fornitori di spazio web e di accesso e degli altri soggetti interessati (società emittenti di carte di credito, responsabili di motori di ricerca…),

— la responsabilità degli autori di software e dei fornitori dei sistemi di sicurezza informatica,

— la protezione delle persone vulnerabili contro le frodi o le informazioni di dubbia attendibilità (truffe di vario tipo, «libera» vendita di sostanze medicinali, terapie o consulenze fornite da persone prive di qualifiche mediche…).

2. **Proposte della Commissione (sintesi)**

2.1 Il programma proposto mira a promuovere un uso sicuro di Internet e delle tecnologie *on-line* per l'utilizzatore finale, in particolare per i bambini ed i giovani, a casa o a scuola. A tal fine, è previsto il cofinanziamento dei progetti, elaborati da associazioni ed altri soggetti (gruppi di ricerca, programmatori di software, istituzioni scolastiche…), volti a consentire lo sviluppo di strumenti di tutela (ad esempio, *hotlines*, sistemi anti-*spam* e programmi antivirus, filtri di navigazione «intelligenti»).

2.2 Il precedente programma per un Internet sicuro (1992-2002) era stato prorogato per il periodo 2003-2004.

2.3 Il sito Internet della Commissione indica i progetti già realizzati nell'ambito del programma *Safer Internet* («Internet più sicuro») fino alla fine del 2003 [1].

2.4 La proposta attuale (2005-2008) si estende altresì ai nuovi mezzi di comunicazione *on-line*: in proposito, essa intende intensificare la lotta ai contenuti illegali e nocivi, ivi compresi i virus e gli altri contenuti dannosi o non richiesti (*spam*).

2.5 Per le istituzioni comunitarie, questa intensificazione della lotta è giustificata una serie di motivi, di cui i principali sono:

— il rapido sviluppo delle connessioni ad alta velocità — sia di lunga durata che permanenti — dei privati, delle imprese, delle amministrazioni e delle organizzazioni private (ONG),

— la diversificazione dei mezzi e metodi di accesso ad Internet e a nuovi contenuti *on-line*, molti dei quali non richiesti (*e-mail, SMS*), nonché la maggiore capacità di attrazione dei contenuti disponibili (multimedialità),

— la vertiginosa espansione dei contenuti non richiesti e potenzialmente nocivi o inopportuni, che comporta nuovi pericoli per il pubblico in generale (virus: invasione degli spazi di memoria, «distrazione» o distruzione di dati, impiego non autorizzato dei mezzi di comunicazione della vittima; messaggi non richiesti (*spam*): utilizzo abusivo della banda passante (larghezza di banda) e delle memorie (di massa), invasione delle caselle di posta elettronica (la cui capacità è spesso limitata), il che impedisce o disturba un uso efficiente di Internet e delle comunicazioni e determina costi notevoli, non sostenuti dai mittenti dei messaggi indesiderati bensì dall'utilizzatore finale). A nuovi pericoli sono esposte poi determinate certe categorie sensibili di utilizzatori, come i bambini (*spam* dagli espliciti contenuti sessuali, messaggi sconvenienti e richieste d'incontro da parte di pedofili nelle aree riservate alla discussione diretta fra utenti (*chat room*)),

— i contenuti non appropriati cui i bambini hanno facilmente accesso a causa della scarsa efficacia delle tecnologie di filtraggio attualmente a disposizione di quanti hanno, appunto, la responsabilità di bambini.

2.6 Il programma è principalmente destinato a proteggere i bambini e coloro che ne hanno la responsabilità (genitori, insegnanti, educatori, ecc.) o difendono i loro interessi sotto il profilo morale o materiale. Il programma coinvolge inoltre le ONG attive nei seguenti ambiti: settore sociale, diritti dell'infanzia, lotta al razzismo, alla xenofobia [2] e ad ogni altra forma di discriminazione, tutela dei consumatori, difesa dei diritti civili, etc.

2.7 Esso tocca inoltre da vicino i governi, le autorità legislative, giudiziarie e di pubblica sicurezza, nonché le autorità di regolamentazione. È necessario adeguare la normativa sostanziale e processuale, come pure formare e dotare di mezzi un numero sufficiente di addetti.

2.8 Il programma interessa altresì l'industria, che necessita di un ambiente sicuro per accrescere la fiducia dei consumatori.

2.9 Le università e la ricerca possono illustrare l'uso che i bambini fanno dei nuovi media. Il modo migliore per convogliare i messaggi relativi alla sicurezza è quello di rendere noti su questi mezzi di comunicazione i modi di procedere dei criminali, di cercare nuove soluzioni tecniche, e di fornire un punto di vista indipendente sul contemperamento degli interessi coinvolti nelle procedure di regolamentazione ed autoregolamentazione.

2.10 Il programma presenta un duplice profilo. Sul piano sociale, esso investe principalmente settori in cui la regolamentazione e il mercato non sarebbero da soli sufficienti a garantire la sicurezza degli utilizzatori. Sul piano economico, esso cerca di promuovere l'uso sicuro di Internet e delle tecnologie *on-line*, stabilendo un clima di fiducia.

2.11 È previsto un finanziamento di circa 50 milioni di euro per potenziare gli strumenti tecnici e giuridici, il software e l'informazione, onde contrastare più efficacemente le intrusioni nelle reti e nei terminali o il loro uso fraudolento per mezzo di messaggi recanti contenuti indesiderati e potenzialmente nocivi sul piano morale, sociale od economico.

[1] http://www.europa.eu.int/information_society/programmes/iap/index_en.htm (sito disponibile unicamente in inglese).

[2] Tali temi avevano formato oggetto di una precedente richiesta del Comitato.

3. **Osservazioni generali del Comitato**

3.1 Il Comitato richiama le posizioni espresse in precedenza con riguardo alla tutela dei minori sulla rete Internet ed al primo programma ([1]). Esso accoglie con favore la proposta di un nuovo programma di lotta ai contenuti illegali o nocivi nelle comunicazioni *on-line* (v. sezione 1. Sintesi, all'inizio del presente documento) ed assicura il suo sostegno agli obiettivi e alle priorità del programma Safer Internet Plus, poiché si tratta di un meccanismo destinato a migliorare la sicurezza su Internet. Il Comitato tiene d'altro canto a far presente l'ampiezza del problema e la particolare esigenza d'iniziative a livello internazionale e di regolamentazioni per contrastare il fenomeno.

3.2 La rete Internet e le nuove tecnologie di comunicazione *on-line* (ad esempio, la telefonia mobile o i PDA con funzioni multimediali e in grado di connettersi in rete, in piena espansione) costituiscono, ad avviso del Comitato, strumenti fondamentali per lo sviluppo dell'economia della conoscenza, dell'*e-economy* e dell'amministrazione *on-line*. Essi sono strumenti proteiformi di comunicazione, di trasmissione di cultura, di lavoro e di divertimento. È quindi fondamentale garantire la sicurezza e la continuità di funzionamento delle reti di comunicazione, poiché si tratta di un servizio pubblico essenziale che deve restare aperto e accessibile e di cui tutti gli utenti devono potersi fidare, affinché sia in grado di svolgere le sue molteplici funzioni nelle migliori condizioni possibili. Uno dei sistemi più utili per comunicare con un gran numero di persone, in base a una valutazione del rapporto costo-efficacia, consisterebbe nel completare l'informazione sull'uso sicuro d'Internet nell'ambito dei diversi programmi e-Europe, specie sul fronte della formazione.

3.3 La libertà di espressione e comunicazione che regna su Internet è agevolata dai costi relativamente modesti delle connessioni, ivi comprese quelle ad alta velocità, che consentono un accesso sempre più agevole ai contenuti multimediali. Solo alcuni paesi poco democratici pretendono di controllare le comunicazioni e i contenuti teoricamente disponibili per i loro cittadini, al prezzo di una costante violazione delle libertà individuali. Il Comitato ritiene che si debba garantire una maggiore sicurezza, salvaguardando e promovendo nello stesso tempo le libertà di informazione, di comunicazione e di espressione.

3.4 Tuttavia, come avviene anche per gli altri mezzi di comunicazione, questo spazio di libertà di espressione e d'informazione costituito da Internet è altresì utilizzato per attività illegali come la pedofilia o la diffusione di contenuti razzisti e xenofobi. Determinati contenuti, come, appunto, la pornografia o i giochi d'azzardo (questi ultimi sono peraltro persino vietati in alcuni paesi) e svariate attività criminali (uso indebito della banda passante o uso fraudolento di dati e di *server*), possono anche rivelarsi nocivi per determinati utenti e in particolare per i minori. Il Comitato approva quindi l'ampliamento del programma all'insieme dei mezzi di comunicazione elettronica suscettibili di accesso non sollecitato o ostile da parte di terzi.

3.5 La regolamentazione di questo nuovo spazio in piena crescita è resa complessa dal suo carattere di rete internazionale aperta e accessibile a tutti a partire da qualsiasi *server* o *client* liberamente connesso da ogni paese del mondo. Numerosi paesi, tuttavia, hanno legislazioni inadeguate o che non funzionano a dovere, e ciò consente a siti vietati nell'Unione europea di proseguire le loro attività. È molto importante che l'Unione europea si pronunci, e si attivi, a favore di un'azione internazionale, segnatamente di concerto con i principali paesi in cui le connessioni Internet a banda larga hanno ampia diffusione, nell'America settentrionale e in Asia. Ciò al fine di proteggere i soggetti più vulnerabili e contrastare più efficacemente l'invio di contenuti non sollecitati (*spam*), i quali mettono a repentaglio lo sviluppo delle comunicazioni via e-mail, nonché la propagazione di virus, che insidia l'economia digitale. Occorre mettere a punto strumenti adeguati capaci di affrontare questi problemi nel contesto non solo comunitario, ma anche e soprattutto globale.

3.6 Nella misura in cui non esistano accordi internazionali, il divieto di certi contenuti in determinati paesi può anche formare oggetto di un ricorso avanti all'OMC, nell'ambito dei TBT ([2]) (Accordi sugli ostacoli tecnici agli scambi), e questo aspetto potrebbe essere trattato nel quadro dei negoziati in corso.

3.7 Il principio di territorialità del diritto e la diversità delle normative nazionali costituiscono un problema difficile da risolvere. Lo stato della tecnologia consente inoltre alle persone di scambiarsi direttamente *files* di ogni natura (*P2P, peer to peer*), ivi compresi *files* criptati il cui contenuto non è controllabile. Ogni macchina o rete *on-line* può essere utilizzata per memorizzare e inviare contenuti sempre più sofisticati, ed è possibile connettersi ad ogni *server* in modo anonimo e non tracciabile, nonché impiegare metodi crittografici estremamente resistenti alla decrittazione o addirittura impossibili da decrittare.

3.8 La moda dei siti personali e degli *weblog*, lo sviluppo dei siti di *e-commerce* o servizi finanziari elettronici, e la moltitudine di siti d'informazione, educativi, scientifici o tecnici, ma anche pornografici o di giochi d'azzardo, etc., fanno sì che nel mondo esistano centinaia di milioni di siti web. Un certo controllo è peraltro possibile grazie alla creazione di indici di parole chiave da parte dei motori di ricerca. I fornitori di accesso ad Internet possono inoltre controllare la creazione di connessioni dirette e di siti preposti all'invio automatico di contenuti, come i messaggi non richiesti (*spam*): la pubblicità commerciale ed altri contenuti non richiesti così inviati possono avere carattere nocivo in generale (uso indebito della banda passante, virus) o in particolare per determinati destinatari come i bambini (cui possono arrecare pregiudizio sul piano morale o psicologico).

([1]) Pareri del CESE sul tema «Programma di protezione dei minori su Internet» (relatrice: DAVISON), GU C 48 del 21.2.2002, in merito alla «Comunicazione della Commissione al Parlamento europeo, al Consiglio, al Comitato economico e sociale europeo e al Comitato delle regioni - Sicurezza delle reti e sicurezza dell'informazione: proposta di un approccio strategico europeo» (relatore: RETUREAU), GU C 48 del 21.2.2002 e sul tema «Libro verde sulla tutela dei minori e della dignità umana nei servizi audiovisivi e di informazione» (relatrice: BARROW), GU C 287 del 22.9.1997.

([2]) «Technical Barriers to Trade». Accordi per la rimozione delle barriere non tariffarie, bensì di carattere tecnico, agli scambi e alle prestazioni di servizi. Cfr. ad esempio la controversia in materia di giochi d'azzardo *offshore* che oppone gli Stati Uniti ad Antigua e Barbuda: il lodo emesso dal collegio arbitrale incaricato di dirimerla è stato impugnato dinanzi all'OMC (http://www.wto.org/french/tratop_f/dispu_f/distabase_wto_members1_f.htm), documento 03-4429, n. WT/DS285/3, del 26 agosto 2003. Il procedimento di appello è tuttora in corso.

3.9 La rete Internet è utilizzata da organizzazioni di tipo mafioso, truffatori, autori di virus, pirati informatici, persone dedite allo spionaggio industriale ed altri delinquenti per svolgervi le proprie attività criminose. La repressione del crimine informatico non è affatto agevole, anche se in molti paesi esistano alcuni servizi speciali delle forze di polizia incaricati di identificare e localizzare questi criminali onde perseguirli penalmente e porre fine alle attività criminose accertate. In genere ciò presuppone una cooperazione a livello internazionale che sarebbe opportuno promuovere maggiormente.

3.10 Come contrastare attività criminose come quelle intraprese mediante siti per pedofili? Se da un lato il loro divieto non pone, né deve porre, alcuna difficoltà sul piano giuridico, dall'altro occorre apprestare i mezzi per localizzare i responsabili nella rete. Come proteggere anche i bambini dai pedofili che agiscano nelle *chat room* — particolarmente apprezzate dai giovani — per cercare di ottenere appuntamenti? In questi casi particolari, il dibattito non verte insomma sulla legittimità del divieto e della repressione, bensì sui mezzi da predisporre per la loro attuazione.

3.11 I fornitori di spazi web e di accesso ad Internet (FAI) non possono sorvegliare e controllare tutti i siti che essi «ospitano» e tutte le comunicazioni dei loro utenti (le quali costituiscono corrispondenza privata). Per contro, su eventuale richiesta della magistratura o della polizia, oppure di un servizio abilitato alla protezione dell'infanzia, i FAI devono ottemperare immediatamente alle richieste o decisioni riguardanti la chiusura di tali siti e l'identificazione delle persone che li utilizzano. Ciò implica la necessità di conservare per un congruo periodo di tempo informazioni concernenti l'immissione di contenuti in rete e le connessioni ai siti.

3.12 Tuttavia, servendosi di indizi quali determinate parole chiave o certe ubicazioni geografiche, le società emittenti di carte di credito, i responsabili dei motori di ricerca e i fornitori di accesso alla rete dovrebbero effettuare controlli (ad esempio su campione) volti a rintracciare siti web legati alla pedofilia, o i cui contenuti siano comunque penalmente illeciti, e riferire alla polizia sull'esito delle loro ricerche. Gli stessi metodi dovrebbero essere utilizzati per identificare i «clienti» che ordinano, mediante carte di credito, pornografia infantile «su misura» o *snuff movies* ([1]). Ove necessario, tali controlli andrebbero imposti per legge. I responsabili dei motori di ricerca dovrebbero inoltre rendere più difficile per gli utenti che navigano nella rete il reperimento su Internet di pornografia infantile o di altri contenuti penalmente illeciti per mezzo di determinate parole o espressioni chiave.

3.13 Tutto ciò presuppone inoltre, da parte delle autorità pubbliche, il ricorso a strumenti di contrasto idonei, a personale qualificato, a una cooperazione transfrontaliera generalizzata e a normative equilibrate a livello nazionale, comunitario ed internazionale, che non incidano sulle libertà di coloro che navigano su Internet, consentendo al contempo di rendere inoffensivi gli individui e le organizzazioni che utilizzano tali reti per trasmettervi contenuti illegali e di bloccare volontariamente la ricezione dei contenuti inopportuni o nocivi.

3.14 Analogamente, per essere efficace, questa azione di contrasto deve coinvolgere direttamente tutti gli utenti di Internet, i quali devono essere formati ed informati sulle precauzioni da adottare e sui mezzi da impiegare per premunirsi contro la ricezione di contenuti nocivi o indesiderati, o per evitare di essere utilizzati come intermediari di tali contenuti. A giudizio del Comitato, la parte del programma relativa alla formazione e all'informazione deve quindi accordare assoluta priorità al coinvolgimento degli utenti, al fine di responsabilizzarli per la loro condotta e per quella dei loro dipendenti. Ad esempio, un problema è costituito dai siti, dedicati a temi inerenti alla salute, che non sono soggetti ad una regolamentazione. Per proteggersi, le imprese devono parimenti curare la formazione del proprio personale e provvedere alla sicurezza delle proprie reti aziendali nonché dei propri siti di commercio elettronico; ma anche le amministrazioni ed istituzioni pubbliche e private devono ricorrere alle medesime politiche di sicurezza e garantire l'assoluta riservatezza dei dati trattati, in particolare di quelli personali. Di pari passo con una maggiore sensibilizzazione, si dovrebbe incoraggiare la messa in rete di contenuti di qualità, nonché invogliare alla pratica di attività sane *off-line* in alternativa alla navigazione prolungata su Internet o alla partecipazione a determinati giochi di ruolo, che alla lunga possono avere effetti negativi su talune personalità immature.

3.15 Gli utenti devono poter disporre dei mezzi idonei a segnalare, presso appositi *call center*, organismi riconosciuti o servizi speciali delle forze di polizia, i contenuti illegali da essi riscontrati nella rete, ed avvertire così i pubblici poteri affinché questi adottino, se necessario, provvedimenti adeguati. I genitori andrebbero messi in guardia nei paesi in cui è frequente lo sfruttamento dei bambini ai fini della pornografia su *Internet* e altri supporti tecnologici, ad esempio alle frontiere esterne dell'Unione. Iniziative del genere potrebbero essere comprese in alcuni programmi di cooperazione RELEX.

3.16 Il Comitato approva gli obiettivi specifici del programma (possibilità per gli utenti di segnalare, attraverso *hotline*, contenuti illegali; sviluppo di tecnologie efficaci di filtraggio di contenuti indesiderati; adeguamento dei sistemi di classificazione dei contenuti; lotta allo *spam*; sostegno alle azioni di autoregolamentazione dell'industria e diffusione della conoscenza dell'uso sicuro delle tecnologie). Nelle sue osservazioni particolari, il Comitato suggerisce alcuni obiettivi ulteriori che ritiene utile siano presi in considerazione.

4. **Osservazioni particolari del Comitato**

4.1 In precedenza il Comitato aveva già chiesto alla Commissione di ridurre gli eccessivi fardelli burocratici imposti dai programmi finanziati dall'UE, in particolare al fine di agevolare l'accesso al finanziamento di microprogetti o di ONG locali. Esso appoggia l'idea di un monitoraggio che si concentri sui risultati tangibili conseguiti grazie al programma e sull'efficacia delle soluzioni proposte, la cui divulgazione dovrebbe essere sottoposta a minori restrizioni.

4.2 Secondo il Comitato, dei provvedimenti normativi a favore della protezione degli utenti finali dovrebbero essere presi in considerazione nel quadro del programma in esame o, se ciò non è possibile, da un'eventuale nuova iniziativa della Commissione.

([1]) Pellicole in cui gli omicidi, le torture e gli altri gravi atti di violenza filmati sono reali.

4.3 Occorre coinvolgere appieno la responsabilità degli autori di software di accesso ad Internet, di sistemi operativi dei *server* o di sistemi per contrastare le intrusioni. Per parte loro, gli utilizzatori dovrebbero avere la garanzia che tali autori di software si avvalgano delle migliori tecniche disponibili e aggiornino regolarmente i loro prodotti. Le garanzie offerte ai clienti dovrebbero essere rafforzate mediante disposizioni di autoregolamentazione e, in mancanza di queste, da una disciplina comunitaria.

4.4 I fornitori d'accesso dovrebbero proporre — e molti di loro di fatto già propongono — l'adozione di strumenti di facile impiego per contrastare i virus a partire dal sito (ancor prima, cioè, che essi infettino i messaggi di posta elettronica o *files* ad essi allegati), nonché di strumenti di filtraggio preliminare della posta elettronica contro gli *spam*. Ciò può assicurare un vantaggio commerciale ai fornitori che si sforzano seriamente di proteggere i loro clienti. Dato che, quando si tratta di Internet, i bambini tendono a essere più intraprendenti dei genitori, è indispensabile preinstallare filtri specifici per la posta e sistemi per l'eliminazione dei virus, la protezione contro le intrusioni e il controllo parentale che possano essere utilizzati e gestiti facilmente da persone prive di particolari conoscenze tecniche.

4.5 Il programma dovrebbe altresì promuovere la ricerca sui software specializzati e gli altri strumenti di verifica dell'«impenetrabilità» del codice macchina dei diversi software di sicurezza e protezione ed incoraggiare o eventualmente obbligare i fornitori a rendere rapidamente disponibili le *patches* (correzioni) volte a rimediare ai difetti, che consentirebbero intrusioni, constatati o segnalati nei programmi e a sviluppare l'efficacia di *firewall* hardware e software come pure i metodi di filtraggio e d'identificazione dell'origine effettiva dei contenuti.

4.6 Il Comitato gradirebbe che gli fosse fornita una valutazione dell'efficacia e dei risultati ottenuti nell'ambito del precedente programma Safer Internet, classificati per categoria di problemi affrontati. Occorrerebbe inoltre dare maggiore diffusione a questo tipo di valutazioni e assicurarsi che vengano mantenuti attivi, e siano meglio conosciuti dai destinatari, tutti i *link* che riguardano i progetti finanziati. Allo scopo di diffondere le conoscenze e promuovere gli scambi o le cooperazioni utili, il sito della Commissione dovrebbe inoltre informare sulle iniziative assunte e le esperienze acquisite negli Stati membri o in paesi terzi.

4.7 È perfettamente possibile intraprendere azioni legali. I fornitori di spazi web e di accesso ad Internet (FAI), le società che emettono carte di credito e i motori di ricerca possono essere tutti soggetti a regolamentazione, e taluni hanno già adottato il sistema dell'autoregolamentazione. Le sanzioni penali contro i siti che promuovono il terrorismo, il razzismo, il suicidio o la pornografia infantile dovrebbero essere pesanti e dissuasive. Occorre attivarsi maggiormente a livello internazionale per identificare e localizzare tali siti onde ottenerne la chiusura nel maggior numero possibile di casi e, ove ciò non sia possibile, avviare negoziati a tale scopo con i paesi dove si trovano i relativi *host*.

5. **Conclusioni**

Pur appoggiando il proseguimento e l'ampliamento del programma «Safer Internet Plus», il Comitato ritiene che il rischio di abusi, soprattutto nei confronti dei bambini, sia talmente grave e di tale portata da richiedere interventi legislativi urgenti e complementari, nonché, tra le altre, misure pratiche dei seguenti tipi:

— previsione dell'obbligo generale, per tutti gli operatori interessati, di proteggere i bambini e, più in generale, gli utenti, in particolare i più vulnerabili,

— installazione automatica («per default») di filtri,

— apposizione di messaggi chiari di sicurezza su tutte le pagine iniziali (*home pages*) e i portali di accesso alle *chatrooms,*

— sostegno alle associazioni che creano linee dirette (*hotlines*) per la segnalazione di siti e attività *on-line* molto dannosi per i bambini,

— divieto dell'uso di carte di credito per ordinare pornografia infantile e altri contenuti criminosi disponibili su Internet, o per operazioni di riciclaggio di denaro sporco,

— segnalazioni e attività mirate dirette a genitori ed educatori, nonché alle autorità dei paesi in cui gli abusi nei confronti di bambini a scopi pornografici costituiscono un problema preoccupante,

— ulteriori interventi nei casi in cui s'instaurino legami fra lo sfruttamento dei bambini a scopi pornografici e il crimine organizzato,

— introduzione di sistemi d'identificazione e informazione sui contenuti nocivi e di soppressione dei contenuti razzisti, diffusione d'informazioni sui tentativi di truffa o sulla vendita di sostanze pericolose per la salute mediante Internet, per proteggere le persone vulnerabili o male informate,

— ricerca, a livello internazionale, di metodi di cooperazione e regole comuni per contrastare più efficacemente lo *spam*,

— cooperazione a livello internazionale (migliorando il sistema di segnalazione tempestiva) e previsione di sanzioni penali dissuasive per quanti diffondono virus informatici e utilizzano illecitamente le reti private e pubbliche per scopi criminosi (intrusioni per occupare la rete a scopi di spionaggio industriale, utilizzo abusivo di banda passante o di altro tipo).

Bruxelles, 16 dicembre 2004.

La Presidente

del Comitato economico e sociale europeo

Anne-Marie SIGMUND