**COMMISSIONE PARLAMENTARE**
**PER L'INFANZIA**

# RESOCONTO STENOGRAFICO

## INDAGINE CONOSCITIVA

**6.**

# SEDUTA DI GIOVEDÌ 7 FEBBRAIO 2002

PRESIDENZA DEL PRESIDENTE **MARIA BURANI PROCACCINI**

# COMMISSIONE PARLAMENTARE PER L'INFANZIA

# RESOCONTO STENOGRAFICO

## INDAGINE CONOSCITIVA

## 6.

# SEDUTA DI GIOVEDÌ 7 FEBBRAIO 2002

PRESIDENZA DEL PRESIDENTE **MARIA BURANI PROCACCINI**

## INDICE

**La seduta comincia alle 14,15.**

*(La Commissione approva il processo verbale della seduta precedente).*

**Sull'ordine dei lavori.**

CARLA CASTELLANI. Chiedo di parlare sull'ordine dei lavori.

PRESIDENTE. Ne ha facoltà.

CARLA CASTELLANI. Vorrei rendere noto a tutti i componenti della Commissione che ho ricevuto ieri mattina un comunicato stampa da parte del professor Antonio Marziale, responsabile dell'Osservatorio sui diritti dei minori, il quale chiede autorevolmente a questa Commissione di dare un segnale rispetto a quanto sta accadendo in Svezia, dove si sta elaborando una normativa che prevede la possibilità per le coppie omosessuali – lo dico con grande rispetto – di adottare bambini. In tale normativa – sulla scorta del fatto che già alcune coppie hanno bambini con loro – si definisce un diritto di questi ultimi l'essere allevati anche da coppie omosessuali.

Non so se la Svezia abbia recepito il trattato di New York sui diritti dell'infanzia e so perfettamente che ogni nazione può legiferare come meglio crede; penso anche, però, che questa Commissione – che così autorevolmente si interessa di problematiche riguardanti l'infanzia – debba dare un segnale al riguardo. So che questa non è la giornata adatta, visto che siamo in procinto di svolgere audizioni molto importanti; le chiedo tuttavia, presidente, di impegnare la Commissione affinché si pronunci al più presto su questo tema.

PRESIDENTE. Onorevole Castellani, nel ringraziarla per il suo intervento sottolineo che in alcuni atti dell'Unione europea sono contenute indicazioni sul modo in cui gli Stati debbano legiferare in materia di infanzia e di adolescenza. Ferma restando la libertà di ogni Stato di adottare le proprie normative, ritengo potrebbe essere utile – al fine di comprendere quali iniziative la nostra Commissione possa assumere al riguardo – disporre del quadro di insieme delle posizioni che l'Unione europea ha espresso e che gli Stati membri dovrebbero rispettare nella stesura di eventuali normative in tema di infanzia e di adolescenza. I nostri uffici svolgeranno un approfondimento al riguardo in modo da fornire alla Commissione un'adeguata base di partenza per eventuali iniziative che decideremo di assumere.

Accolgo quindi volentieri la sua richiesta di sottoporre al più presto all'attenzione della Commissione questo argomento.

**Sulla pubblicità dei lavori.**

PRESIDENTE. Avverto che, se non vi sono obiezioni, la pubblicità dei lavori sarà assicurata anche mediante l'attivazione dell'impianto audiovisivo a circuito chiuso.

*(Così rimane stabilito).*

**Audizione dell'ingegner Paolo Nuti, Presidente dell'Associazione italiana Internet providers e del dottor Matteo Fici, Presidente dell'Assoprovider, in relazione alla problematica della regolamentazione di Internet.**

PRESIDENTE. L'ordine del giorno reca, nell'ambito dell'indagine conoscitiva sull'abuso e lo sfruttamento dei minori, l'au-

dizione dell'ingegner Paolo Nuti, presidente dell'Associazione italiana Internet *providers* e del dottor Matteo Fici, presidente dell'Assoprovider, in relazione alla problematica della regolamentazione di Internet. Comunico che il dottor Fici è accompagnato da don Ilario Rolle, rappresentante dell'Assoprovider.

Ringrazio i nostri ospiti per la loro presenza e do senz'altro la parola all'ingegner Paolo Nuti, al quale chiederei di illustrare in particolar modo le opportunità che si presentano nell'utilizzo di Internet da parte di adolescenti e famiglie, le modalità per prevenire intrusioni e le strategie a suo avviso migliori per raggiungere l'obiettivo di un uso sicuro del mezzo informatico sia da parte dei ragazzi che delle loro famiglie. Ci interessano anche i possibili interventi attuabili presso gli operatori che lavorano nelle scuole.

PAOLO NUTI, *Presidente dell'Associazione italiana Internet providers.* Ringrazio il presidente e tutti i componenti la Commissione per l'opportunità che ci è stata offerta. La materia di cui parliamo è molto complessa; ho visto che la Commissione ha svolto altre audizioni e quindi molti problemi sono già noti. Cercherò pertanto di trattare singoli punti più che affrontare un discorso strutturato, anche per esigenze di rapidità.

In sostanza, i problemi della tutela dei minori rispetto ad Internet possono ricondursi a due grandi categorie. La prima riguarda la necessità di evitare il contatto del minore con contenuti illegali o sensibili (cioè inadatti al minore) ed altre forme dirette di abuso a suo danno, quali ad esempio l'adescamento mediante *chat line* o forme di plagio, la raccolta di dati riservati sulla famiglia, i condizionamenti pubblicitari, eccetera.

La seconda grande categoria di problemi concerne le modalità per reprimere ogni forma di abuso e sfruttamento dei minori e, più in generale, di ogni attività criminosa *on line*: è quello che in gergo chiamiamo *computer crime*. Le tecniche e gli strumenti per raggiungere questo obiettivo sono sostanzialmente unificabili con quelli richiesti dall'obiettivo più ampio.

Articolerò la mia esposizione in una panoramica degli strumenti a disposizione della famiglia e dell'educatore per tutelare il minore ed in un esame delle problematiche e dei mezzi necessari per raggiungere il secondo obiettivo, vale a dire combattere il *computer crime*.

Trattando gli strumenti atti ad evitare il contatto dei minori con contenuti illegali o sensibili ed ogni altra forma di abuso, si deve effettuare una distinzione in due classi. La prima riguarda gli strumenti installabili direttamente sul *computer* dell'utente (cioè da parte dei genitori nei confronti del minore); la seconda concerne invece gli strumenti che possono essere messi a disposizione della famiglia da parte dei fornitori di servizi.

Alla prima categoria appartengono mezzi che immagino conosciate benissimo. Il primo è costituito dalla marcatura di sensibilità dei contenuti posto a cura dell'autore (in gergo PICS). Il pregio di questa soluzione è di essere subito disponibile nella misura in cui tutti i principali *browser* consentono di abilitare la modalità di controllo a mezzo PICS. I difetti sono rappresentati dal fatto che la definizione di « contenuti sensibili » varia da zona a zona, da cultura a cultura, da famiglia a famiglia, per cui un'armonizzazione risulta difficile; in secondo luogo, questo sistema sbarra tutti i contenuti non marcati: pertanto, se gli autori di determinati contenuti non abbiano ritenuto rilevante predisporre una marcatura affinché gli stessi fossero visibili ai minori, non saranno visibili in assoluto. Il terzo difetto – che tutto sommato non è da poco – è che se navighiamo in Internet ci accorgiamo che i fornitori di contenuti sensibili si preoccupano moltissimo di attivare il PICS, mentre gli altri trascurano questo aspetto, per cui il tutto appare – scusate il termine – una foglia di fico.

La seconda metodologia consiste nel prevedere filtri di navigazione, tra i quali possono essere enucleati quelli che operano sulla base di *black list* (direi che sono i più diffusi). Queste ultime possono essere redatte manualmente o automaticamente;

nel primo caso hanno il valore aggiunto della redazione. Il pregio principale è rappresentato dalla consistenza delle indicazioni; i difetti sono l'incompletezza delle stesse, il costo di mantenimento di questa base dati di siti sbarrati (costo che a mio avviso potrebbe essere oggetto di una qualche forma di aiuto statale), le censure arbitrarie, la responsabilità civile del fornitore e le clausole di limitazione della responsabilità stessa. Queste ultime – poiché il fornitore non riesce ad assumersi la responsabilità di eventuali incompletezze della lista – comportano che egli avvisi l'utente, cioè la famiglia, della limitazione della responsabilità.

L'alternativa ad una *black list* redatta manualmente è costituita da un filtro automatico, con tutti i relativi problemi, soprattutto l'incertezza delle indicazioni (falsi positivi e falsi negativi). Lascio a disposizione della Commissione una documentazione contenente esempi pratici di applicazioni: funzionano su questo principio *Cyber patrol*, *Cyber sentinel* ed anche altri programmi.

L'altra classe di servizi che può essere installata sul PC dell'utente è il monitoraggio della navigazione. Qualunque operazione venga effettuata sul *computer* resta memorizzata per periodi più o meno lunghi (dipende dallo spazio presente sull'*hard disk* e da altri elementi) nelle cosiddette *cache*, vale a dire memorie temporanee. Un esperto, senza ricorrere ad altri *software*, è in grado di ricostruire buona parte dell'attività dell'utente su un certo *computer*. Si tratta di un problema di *privacy*; se lo trasferiamo nell'ambito che ci interessa, grazie a questi strumenti e ad ulteriori implementazioni *software* è possibile registrare l'attività svolta dal minore al *computer*. Sulla base di questo principio funzionano programmi come *ChildSafe*. L'impatto di questa tipologia di programmi (che in sostanza sono spie) deve essere valutato attentamente, non solo nei confronti del minore ma anche degli altri componenti la famiglia, che potrebbero trovarsi indirettamente « spiati ». Come vedete, siamo di fronte al problema generale di conciliare necessità diverse.

Passando alla categoria dei servizi offerti dal fornitore di accesso, essi sono sostanzialmente simili a quelli offerti dai *software* (con l'eccezione della classificazione dei contenuti): accessi condizionati sulla base di *black list* o *white list* (sorvolo sui pregi e difetti che sono sostanzialmente analoghi a quelli visti prima).

Lo strumento corrispondente al programma di monitoraggio dell'attività dell'utente offerto come servizio da un fornitore presenta problematiche di tutela della *privacy* sostanzialmente insormontabili. Pur essendo un aspetto estremamente delicato, nei miei contatti ho colto una certa tendenza a valutare una strada del genere. Cerchiamo di capire di cosa stiamo parlando.

È possibile inserire in tutte le reti (e di fatto ciò avviene proprio al fine di fornire servizi di *white* o *black list* o di accelerazione della velocità di collegamento) macchine chiamate *proxy server*: si tratta di memorie temporanee in cui viene accumulato il traffico svolto dagli utenti; tale traffico viene necessariamente marcato da un numero IP dell'utente che ha richiesto un certo servizio e da un numero IP della destinazione cui quest'ultimo è stato richiesto.

Questi *proxy server* devono, per poter funzionare, avere un *log*, il quale è « a perdere » nel minor tempo possibile. Ciò per una necessità di carattere economico: se dovessimo « loggare » tutti i marcatori dell'attività svolta dall'utente (non parlo dei dati ma della singola azione: « contatta la tale *directory* del tale *server* ») i *log* sarebbero enormi e quindi costituirebbero un onere che non sarebbe congruo con la funzione che i *server* svolgono attualmente. Il fatto che potenzialmente questi *proxy server* siano in grado di svolgere tale servizio può suggerire la possibilità di memorizzare permanentemente presso il *provider* oppure di trasmettere ad un'apposita banca dati centralizzata tutte queste indicazioni.

Se un servizio di tal genere venisse attivato a richiesta espressa dell'interessato sarebbe lecito; ma nel momento in cui attraverso questo servizio passano non solo l'interessato che lo ha richiesto ma anche altri soggetti, si va ad impattare con l'articolo 15 e con l'articolo 21 della Costituzione, nonché, forse, con la legge n. 675 del 1996. Non mi risulta che in pratica vi siano fornitori che offrano un servizio di questo genere, ancorché sia teoricamente realizzabile: su questo « teoricamente » dovremo tornare più tardi.

L'ultimo tipo di servizio offerto dai fornitori consiste nei motori di ricerca filtrati. È un servizio di secondo livello: se il motore di ricerca dei contenuti filtra siti compresi in una *black list* o altri che fanno capo ad una *black list* di parole non ammissibili, certamente l'indicazione per il minore che naviga è ridotta. Nulla impedisce però allo stesso minore di includere un indirizzo, letto su un giornale o altrove, nel *browser*: diciamo quindi che questo tipo di servizio è sostanzialmente inutile.

Tutti i servizi di questo genere hanno problemi comuni: innanzitutto, la difficoltà dei genitori nello scegliere, nell'installare, nel configurare e nel mantenere qualsiasi fra queste soluzioni. Il minore esperto (parliamo di ragazzi di 13 o 14 anni) spesso e volentieri è in grado di aggirare qualsiasi programma del genere, non fosse altro ricostruendo un intero *computer* virtuale sul PC. L'altro problema è che quando si parla di Internet l'opinione pubblica, ma anche qualche addetto ai lavori, pensa al *web*; ma Internet non è solo questo. Abbiamo detto che fortunatamente alcuni di questi programmi consentono di effettuare una sorta di controllo nelle *chat*, sulle *e-mail*, eccetera. Contemporaneamente questi programmi danno al genitore ed alla famiglia un falso senso di sicurezza perché nessuno dei fornitori di queste tecnologie – se è onesto – potrà promettere una certezza di efficacia delle stesse.

Denominatore comune di queste soluzioni è che serve comunque la presenza dell'adulto: Internet non è una *baby sitter* (penso sia già stato detto in questa sede, ma credo che non lo si ripeta mai abbastanza), come non lo è la televisione. Molti problemi sono assolutamente comuni, compreso quello del plagio pubblicitario.

In definitiva, già oggi, per quanto riguarda questa prima categoria di problemi, esiste sul mercato un'ampia gamma di servizi da impostare direttamente sul *computer* o da utilizzare tramite fornitori. Peraltro, debbo rilevare che nonostante l'elevato livello di attenzione dell'opinione pubblica al problema della protezione dei minori in rete, l'utilizzazione dei servizi di accesso controllato ad Internet (è qui presente il responsabile di Davide.it, che è il primo servizio di questo genere realizzato in Italia) è del tutto marginale. Sarebbe quindi auspicabile un'opera di sensibilizzazione delle famiglie circa la disponibilità di tali servizi: mi riferisco ad un intervento di tipo sostanziale, effettuato tramite comunicazione televisiva o quanto meno a mezzo stampa, in quanto su Internet le notizie sulla disponibilità di questi servizi sono moltissime; ciò nondimeno, non sono usati. Comunque, ribadisco che è insostituibile la presenza dell'adulto.

Passo ora a trattare il problema della repressione e prevenzione dei reati informatici e telematici, con particolare riguardo agli abusi a danno dei minori. Diamo per scontato che le principali problematiche sono già state evidenziate; il nostro obiettivo è illustrare quello che a nostro avviso rappresenta un corretto bilanciamento tra i diversi oneri da sostenere.

Esiste anzitutto un principio giuridico che stabilisce chiaramente che la responsabilità penale è assolutamente individuale; ne consegue che l'efficacia dei provvedimenti di repressione di qualunque reato è reale solo se è possibile individuarne l'autore: si può comminare l'ergastolo, ma se non siamo in grado di individuare l'autore del reato tutto si risolve in un nulla di fatto.

Il problema di fondo è allora quello dell'anonimato. Esaminiamo quale gradualità di anonimato possiamo incontrare. Anzitutto c'è l'anonimato totale, invocato

da alcuni in nome della libertà di espressione, che però rende inefficace ogni provvedimento di contrasto del *computer crime*. C'è anche da sottolineare che l'anonimato totale rappresenta un valore economico, perché grazie ad esso lo sviluppo di Internet e del commercio elettronico è certamente più rapido. Il grande sviluppo di Internet attraverso il cosiddetto accesso *free* si è ottenuto passando sopra a questo problema, nelle prime fasi; poi esso è stato sollevato da varie parti – tra cui la stessa associazione che rappresento – e si è arrivati a definire forme di contratto o comunque di mantenimento dei registri dell'accesso ad Internet che in un primo momento sembravano non proponibili ai sensi della legge n. 675 del 1996, mentre poi si è meglio chiarito che si potevano conciliare gli aspetti della sicurezza delle reti e quello dell'autorizzazione all'elaborazione dei dati. Si è trovata una soluzione, adottata dalla maggioranza dei fornitori di accesso, che in buona sostanza consiste nel mantenere un registro di assegnazione temporanea dei numeri di rete, che rappresentano l'elemento chiave per proseguire in quella che definirò come la « catena del freddo » della responsabilità.

Questi registri di assegnazione temporanea riportano normalmente – quando l'utente non lo oscura – l'indicatore del numero di telefono della persona che ha chiamato. Si tratta di un'indicazione fondamentale che, con il senno di poi, possiamo ritenere non costituisca una lesione della *privacy* dell'interessato ma, viceversa, una misura di sicurezza a sua tutela. Sapete infatti che ogni accesso alla rete viene generalmente governato da un codice e da una *password*, attraverso la quale l'utente gode di certi servizi, quali ad esempio la posta elettronica.

Sapere che qualcuno ha utilizzato il mio codice o la mia *password* senza che ne sapessi nulla rappresenta un'informazione fondamentale a mia tutela. Se il fornitore di servizi dà la possibilità di accedere al registro delle chiamate nominalmente fatte da me posso anche verificare se qualche chiamata sia partita da sedi che non conosco: non è una tutela al 100 per cento, ma è sicuramente molto elevata.

D'altro canto, l'informazione mantenuta su questo registro non aggiunge nulla a quella che comunque il fornitore degli accessi possiede in tutti i casi in cui il cliente viene fornito di una linea dedicata. Normalmente c'è un contratto scritto, ma, in ogni caso, per poter fornire un collegamento dedicato e permanente occorre sapere dove abita il cliente: mi riferisco a tutti i clienti collegati a mezzo circuiti diretti numerici (CDN), a mezzo XDSL, a mezzo fibra ottica, che già forniscono contrattualmente questa informazione al *provider*. Possiamo quindi dire, col senno di poi, che la tenuta di quel registro non costituisce una variazione della quantità di informazioni detenuta dal fornitore a disposizione per eventuali indagini successive a carico dell'utente.

Ho anticipato un aspetto centrale della mia esposizione; vorrei ora tornare ad esaminare il problema dell'anonimato. Da un lato c'è l'anonimato totale, mentre all'estremo opposto si colloca la richiesta di nominatività di ogni contenuto o azione. Questo risultato può essere facilmente raggiunto utilizzando la centralizzazione degli archivi *(log)* di accesso ad Internet e di utilizzazione dei servizi, ivi compreso quel servizio di archivio del *proxy* che non deve essere mantenuto secondo la normativa corrente ma che potrebbe esserlo.

Se centralizziamo gli archivi di tutte le attività (assegnazione di IP, navigazione, eccetera), anche se qualcuno può sostenere che mancando l'ulteriore elaborazione « a valle » di questa archiviazione di fatto tutte le informazioni mantenute in questo archivio centralizzato sono anonime (poiché i mezzi informatici agiscono molto rapidamente e talora anche all'insaputa del loro proprietario), si crea un *dossier* informatico relativo a ciascun utente di Internet, conservato per un certo numero di anni. Detto in questi termini, credo che ciò spaventi un po' tutti, oltre ovviamente a violare l'articolo 15 della Costituzione, la legge n. 675 del 1996, eccetera.

L'opinione pubblica è talmente sensibile alla protezione dei minori – giustamente – che è facile cogliere espressioni forti: mi riferisco a quella di un mio amico, peraltro persona di cultura superiore, il quale dice che per proteggere sua figlia di nove anni da un pedofilo sarebbe disposto a cambiare l'articolo 15. Ciò fa parte di una sensibilità promossa dai *media* sulla quale penso che le persone responsabili debbano riflettere a lungo.

La creazione di questo archivio centralizzato comporta un problema non da poco, su cui finora è stata fatta non molta pubblicità, benché la questione sia nota ormai da diversi mesi tra gli addetti ai lavori. La nominatività del contenuto di ogni azione può essere facilmente estesa (e forse sta per essere estesa) al singolo « pacchetto » di dati inviati. È una cosa di per sé incomprensibile: sapete che su Internet le informazioni viaggiano in « pacchetti » di 256 *byte*, smistati sulla base dell'indirizzo di provenienza e di destinazione, eccetera.

Si stanno verificando due eventi. Il primo è certo: è stato introdotto sul mercato da parte del più grande produttore di sistemi operativi del mondo (cioè la Microsoft) un nuovo sistema operativo, chiamato XP, che richiede che l'utente iscriva le caratteristiche tecniche del proprio *computer* presso un archivio centralizzato della Microsoft stessa. Se si installa XP sul *computer* esso funziona per 15 giorni; se voglio che il funzionamento prosegua, devo far calcolare ad un apposito *software* di registrazione un numero particolare, chiamato *global user identifier*, specifico del singolo *computer*, nel senso che viene calcolato dal *software* sulla base del contenuto (tipo di processore, scheda video, numero di matricola del programma acquistato, eccetera). Di fatto, si tratta di un numero unico per ciascun *computer*. Questo numero viene inviato al produttore negli Stati Uniti ed archiviato; il tutto fa parte di un sistema di difesa dalle copie abusive di *software*. È comprensibile, ma su questo archivio centralizzato, collocato oltre tutto in un paese esterno alla comunità europea, ci sarebbe da fare qualche riflessione.

Già a partire da agosto sono apparsi articoli – che per la prima metà si sono dimostrati *a posteriori* assolutamente corrispondenti al vero – che hanno illustrato questa evoluzione di Internet: nominatività del singolo pacchetto TCP/IP ottenuta inserendo in alcuni *byte* liberi del pacchetto il GUI, vale a dire questo numero di matricola di cui si sta creando il registro.

Il punto è: perché dovrei usare questo pacchetto TCP/IP modificato invece di quello *standard*? Semplice: perché la catasta TCP/IP che utilizzo normalmente diventa insicura e inizia a funzionare male. In altre parole, rendendo debole dal punto di vista della sicurezza informatica il protocollo *standard* normalmente utilizzato da tutti si può « spingere » il pubblico a cambiare tipo di protocollo per sceglierne uno più sicuro, che però obbliga ad una globalizzazione dell'archivio.

Questo aspetto – anche se esula dal tema che ci sta a cuore – deve essere a mio avviso tenuto presente nell'ambito di una considerazione più ampia sul bilanciamento tra gli oneri di persecuzione del *computer crime* ed il rispetto delle libertà individuali.

Tra l'anonimato totale e le possibili forme di nominatività di ogni singola azione esiste una forma intermedia, quella che da diversi anni ormai gli addetti ai lavori definiscono « anonimato protetto ». Con questa espressione si intende la distribuzione fra i diversi fornitori del servizio di informazioni anonime che restano tali fino a quando – su espresso provvedimento dell'autorità giudiziaria – non si richiede il collazionamento di tutti questi pezzi di informazione che iniziano con un IP e terminano con un altro IP. Queste informazioni non devono essere conservate in un unico archivio, per evitare la « dossierizzazione », e quindi devono essere distribuite tra i vari fornitori. Bisogna poi individuare quali informazioni servono, per quanto tempo devono essere mantenute e come. Nella corretta esecuzione delle modalità di mantenimento di

tali informazioni dovrebbe essere concentrata la responsabilità del singolo fornitore di servizi.

C'è poi da dire che sarebbe opportuno che le informazioni memorizzate per il mantenimento della catena di anonimato protetto fossero congrue. Faccio un esempio. L'unico caso in cui è rilevante assumere informazioni sul fatto che sia stata vista una certa pagina è il reato di accesso a contenuti pedopornografici definito dalla legge n. 269 del 1998. Chi distribuisce questi contenuti compie un reato ancora più grave e si guarda bene dal mantenere un *log* dei *server* di accesso. Imporre quest'ultimo obbligo diventa pleonastico; questi *log* invece vengono inseriti quando – sempre sulla base della legge n. 269 – vengono creati siti civetta.

Per quanto riguarda i contenuti che si trovano all'estero, c'è il problema, che credo sia ben noto alla Commissione, per cui non in tutti i paesi del mondo la pedopornografia è un reato. Bisognerebbe quindi valutare altri aspetti: se le autorità italiane ricevessero il *log* degli accessi, di fatto ciò rappresenterebbe una forma di ricatto dell'utente italiano da parte del fornitore di quel materiale. Si tratta di una questione molto variegata che però non interessa in un'ottica di adozione a breve dell'anonimato protetto. Interessa invece dar vita ad un anonimato protetto ma congruo.

In pratica, l'anonimato protetto corrisponde ad una sorta di « catena del freddo ». Come avviene per i surgelati, ci sono vari anelli rappresentati dai fornitori (quelli di accesso, dei servizi intermedi, di informazione); l'adozione dell'anonimato protetto per ora è parziale nella misura in cui il fornitore di accesso già fa tutto quanto è necessario, mentre i fornitori di altri servizi non sempre si comportano allo stesso modo.

Facciamo un esempio che capita abbastanza di frequente. La maggior parte delle segnalazioni di importanza minore (anche se per l'interessato sono di importanza assoluta) riguardano il caso della diffamazione: qualcuno ha detto qualcosa di qualcun altro, aggiotaggio e così via. Ciò avviene normalmente attraverso *e-mail* o *newsgroup*. L'utente inesperto di Internet quando riceve un messaggio da un certo destinatario ritiene che sia quest'ultimo ad averglielo inviato. Questo non è necessariamente vero. Appena diventa solo un po' più smaliziato impara subito che i messaggi che invia sono intestati in un certo modo solo perché egli lo ha scritto (o per lui lo ha fatto il suo fornitore di servizi) nel programma di posta elettronica. Sfortunatamente, però, in questo programma si può scrivere qualunque cosa, compreso il nome di un'altra persona. L'utente più smaliziato potrebbe pensare di assumere l'identità di un terzo, ovviamente danneggiandolo. Se lo fa, si mette nei guai, perché crede di aver creato un messaggio anonimo che però tale non è. Qualunque messaggio deve essere inviato attraverso un *server* SMTP; quest'ultimo, nel momento in cui riceve la richiesta del sedicente Paolo Nuti – tanto per fare un esempio – di inviare il messaggio, prende nota del numero IP da cui è partita la richiesta e attribuisce al messaggio un numero identificativo. Questi numeri vengono spediti al destinatario, solo che quest'ultimo non sa che si possono vedere, abilitando il programma di posta elettronica a farlo.

La scarsa conoscenza comporta dunque contemporaneamente che il destinatario sporge una denuncia senza aver raccolto tutte le prove necessarie per rintracciare l'autore della impersonificazione non autorizzata e che, se il destinatario è abile, l'utente di secondo livello compie un reato penalmente rilevante e piuttosto grave. La mancanza di informazione comporta la commissione dei reati; d'altro canto, la « catena del freddo » che ho descritto prima consente di punire il colpevole, posto che da qualche parte si stabilisca l'obbligo di mantenere non il contenuto del messaggio ma il *log* del *server* di posta elettronica per un periodo di tempo variabile e comunque congruo.

È fondamentale identificare i soggetti che operano su Internet e le relative responsabilità. Spesso e volentieri l'utente – normalmente considerato come il sog-

getto che patisce il danno – si trasforma nel fornitore di informazioni. Il fornitore dei contenuti deve essere responsabile dei medesimi, quello di accesso a mio avviso deve sapere a chi ha dato il permesso direttamente o indirettamente, mentre il fornitore di servizi deve essere responsabile di non interrompere quella « catena del freddo » di cui abbiamo parlato prima.

Utilizzando il meccanismo da noi auspicato riusciamo a conciliare le diverse esigenze. L'ultimo problema è quello della rimozione dei contenuti. Questa non può avvenire per iniziativa propria dal fornitore dei servizi, ancorché venga avvisato da qualcuno che i contenuti che sta ospitando per conto di un terzo sono illegali. Questi ultimi, salvo casi plateali, devono essere valutati come tali ed il fornitore di servizi non può trasformarsi in giudice: sarebbe assolutamente improprio. Occorre quindi creare un meccanismo (chiamiamolo *hot line)* che consenta di incanalare con certezza le segnalazioni con un metodo sufficientemente rapido e di attivare qualcuno (una commissione o direttamente il magistrato) che possa immediatamente emettere una ordinanza di sospensione della fornitura del servizio di distribuzione.

Sono già stati realizzati, circa quattro anni fa, due codici di autoregolamentazione, quello dell'ANFOV e quello della AIIP: hanno bisogno di aggiornamento e si è già messo in moto il meccanismo che in brevissimo tempo renderà necessario rinnovare tali codici e presentarli al Garante per la *privacy* per una eventuale pubblicazione sulla *Gazzetta Ufficiale.*

PRESIDENTE. La ringrazio, ingegner Nuti.

GAETANO FASOLINO. Presidente, intervengo per sottolineare che i nostri lavori stanno procedendo in modo assai interessante ma necessitano, a mio avviso, di una razionalizzazione per il futuro.

Dal momento che il tempo previsto per l'audizione, dalle 14 alle 15, è trascorso, credo che oggi non procederemo oltre nei nostri lavori. Dovremmo però fare il punto della situazione dopo l'interessante relazione che abbiamo ascoltato e dar corso anche ad atti concreti. Sorge comunque il problema per tutti noi di raccordare i nostri lavori con quelli delle Assemblee di appartenenza: personalmente desidero dare un contributo partecipando a questa Commissione, ma al tempo stesso non posso evitare di seguire anche le attività che si svolgono al Senato. La invito, presidente, a tener conto di queste difficoltà per evitare che il nostro apporto ai lavori della Commissione diminuisca in misura rilevante.

PRESIDENTE. Anzitutto devo sottolineare che nella convocazione non era previsto un orario finale per la seduta. Comunque, mi rendo conto delle difficoltà da lei sottolineate, senatore Fasolino; credo che una soluzione potrebbe essere quella di inviare a tutti una sorta di questionario al quale vi prego di rispondere. I lavori di Camera e Senato sono quelli che sono e gli orari disponibili li conosciamo. Pochi di voi – ed è giusto che sia così – sono disponibili a venire il lunedì o a rimanere il giovedì; sottolineate che la sera alle 19 o alle 20 tutti sono stanchi e che alle 16 ricomincia l'attività nelle Camere di appartenenza. Anch'io mi trovo nella vostra situazione e ricordo che analoghi problemi si posero nella scorsa legislatura.

Tra l'altro, i nostri ospiti si fanno portatori di informazioni importantissime da cui dovremo prendere spunto per iniziative legislative; per noi è frustrante non riuscire a riservare a queste occasioni l'attenzione che meritano.

GAETANO FASOLINO. Presidente, forse la cosa più importante sarebbe stabilire operativamente, di fronte a relazioni tecniche come quella che abbiamo ascoltato, che sono di notevole valore, un modo per risolvere i problemi citati. Si potrebbe ad esempio prevedere che non tutta la Commissione ma solo un gruppo più ristretto acquisisca le informazioni dai vari settori che ci interessano per enucleare gli spunti per le iniziative legislative di cui lei

ha parlato. Uno dei problemi che mi pongo sovente è di capire in che modo concreto combattiamo il fenomeno della pedopornografia e quali iniziative siano ascrivibili al nostro operato. Dai tecnici, più che una relazione estremamente puntuale e circostanziata, mi aspetto – come avviene a Bruxelles e a Strasburgo – l'esposizione in una decina di minuti di una serie di indicazioni operative con le quali cimentarci. La mia preoccupazione è che, in caso contrario, si ascolti molto e si recepisca abbastanza, ma comunque non in misura sufficiente, perché non tutti i colleghi sono presenti: il rischio è che da una gran mole di informazioni non scaturisca molto in termini di proposte operative.

So che la Presidente è molto esperta del settore e che si farà promotrice, insieme con altri colleghi, di importanti iniziative. Ritengo però che dobbiamo « stringere » sulle audizioni e soprattutto ottenere indicazioni operative per atti legislativi.

PRESIDENTE. Faremo senz'altro tesoro dei suoi suggerimenti, senatore Fasolino. Ad ogni modo, delle audizioni è redatto un resoconto stenografico, che costituisce un supporto importantissimo anche per coloro che per motivi vari – non ultimo la concomitanza dei lavori parlamentari – non possono partecipare direttamente alle sedute. Potranno poi aver luogo riunioni operative per fare la sintesi della situazione.

PIERO PELLICINI. Presidente, vorrei anzitutto dire che non concordo con il riferimento fatto dal senatore Fasolino ai lavori di Strasburgo e di Bruxelles; a Strasburgo sono i politici a parlare poco (tre o cinque minuti), mentre gli esperti sono ascoltati per il tempo necessario.

Vorrei poi manifestare un dubbio che è sorto in me ascoltando la relazione dell'ingegner Nuti. Premesso che l'anonimato protetto è l'unica forma di prevenzione possibile (perché non si può accettare un « grande orecchio » che ascolta tutto né una situazione in cui non si sente niente), è necessario un controllo, che nello Stato di diritto è esercitato dalla magistratura. Ho fatto parte, come ufficiale di complemento, dell'Arma dei carabinieri, anche se solo per qualche mese: un periodo comunque sufficiente per trarre utili insegnamenti. In questo settore è necessario un intervento urgentissimo, che deve provenire dal pubblico ministero: eventualmente il GIP lo convaliderà in un secondo momento. Sono insomma indispensabili una serie di attività di pronto intervento, naturalmente in relazione all'evoluzione dei tempi.

Da quanto ha detto l'ingegner Nuti ho capito che sarebbe possibile che in questo momento un signore che mi ha inviato una *e-mail* e che quindi conosce i miei dati ordini a nome dell'avvocato Piero Pellicini, senatore della Repubblica, una cassetta pornografica, 24 bombe a mano, o altro. È possibile ora che ciò avvenga o sarà possibile che avvenga in futuro ?

Un conto è la tutela della vittima, altro conto è quella di chi è accusato di essere autore di un certo reato. Ho fatto l'ufficiale dei carabinieri e l'avvocato, per cui mi dibatto da una vita tra le esigenze di repressione e quelle di garanzia: mi domando che cosa ci dobbiamo aspettare in questo campo così difficile.

PRESIDENTE. Darei ora la parola al dottor Fici, presidente dell'Assoprovider, per poi passare alle eventuali domande dei colleghi.

MATTEO FICI, *Presidente dell'Assoprovider*. Ho fatto venire con me don Ilario Rolle, che ha maturato un'esperienza specifica che è interessante veicolare in questa sede per capire cosa si possa fare per limitare significativamente l'impatto di queste problematiche.

Volevo comunque dire che in Italia ed in Europa si registra un ritardo nella diffusione di Internet rispetto agli Stati Uniti. Da ciò derivano difficoltà di sviluppo per l'economia complessiva del continente. L'uso di Internet non può essere impedito né limitato nel tempo per i minori: ciò equivarrebbe a fare di questi

ultimi degli analfabeti del futuro. Vengo da Palermo e posso dirvi che dobbiamo comportarci in modo esattamente opposto.

Noi rappresentiamo gli Internet *service provider*, vale a dire le aziende che storicamente hanno fornito collegamenti e servizi Internet prima che in questo settore entrassero pesantemente le compagnie telefoniche. Normalmente con i nostri clienti abbiamo un rapporto che ha consentito a questi ultimi di godere di prodotti e siti *web* di qualità, mentre quando ci si sposta su grandi quantità di abbonamenti – come è avvenuto in seguito all'entrata delle compagnie telefoniche – la qualità subisce uno scadimento.

Le aziende che operano in questo settore stanno, quindi, vivendo gravissimi problemi dovuti al fatto che gli operatori telefonici hanno dimensioni molto maggiori e stanno cercando di farle chiudere dettando regole che falsano sostanzialmente le condizioni della concorrenza. Se gli Internet *service provider* dovessero continuare ad avere problemi o addirittura dovessero chiudere, ciò non aiuterà a risolvere i problemi perché il nostro apporto si pone soprattutto sul piano dell'informazione e dell'alfabetizzazione all'uso intelligente di Internet. Il problema dell'uso di Internet da parte dei minori riguarda sostanzialmente anche la formazione: se il genitore fosse in grado di seguire ciò che suo figlio sta facendo sul *computer* e non accadesse che il figlio è molto più bravo del genitore, probabilmente molti problemi sarebbero risolti; lo stesso accadrebbe se Internet o la televisione non fossero utilizzati come *baby sitter*.

Vi rivolgo un appello affinché dimostriate quanto meno simpatia verso il nostro settore e, qualora se ne presenti l'occasione durante i lavori parlamentari, valutiate con attenzione eventuali provvedimenti che ci riguardino. Vi prego di ricordare che le nostre aziende hanno effettuato l'alfabetizzazione e se ci allontaneremo dal mercato perché devono restare solo i più grossi e prepotenti (consentitemi questa « licenza poetica ») si perderà la vicinanza con l'utente. La formazione secondo me è fondamentale e occorre adottare provvedimenti che favoriscano la comunicazione relativa all'utilizzo di strumenti come quello che ora don Ilario illustrerà rapidamente.

Per il resto mi associo a quanto diceva l'ingegner Nuti. Lascio la parola a don Ilario, che vi racconterà un'esperienza unica, che rischia di non proseguire perché non esistono attualmente provvedimenti che favoriscano situazioni di questo tipo: sarebbe veramente un peccato se ciò accadesse.

PRESIDENTE. Prima di dare la parola a don Ilario Rolle, colgo l'occasione per ringraziare l'ingegner Nuti anche per il materiale che ci ha consegnato, che costituirà una notevole base di lavoro.

ILARIO ROLLE, *Rappresentante dell'Assoprovider*. Vorrei anzitutto ringraziare la Commissione per avermi dato la possibilità di esporre le esperienze che ho vissuto dal 1997 quando, su *input* del cardinale di Torino, ho cominciato ad occuparmi dell'educazione dei minori all'uso della rete.

Consultando i colleghi americani mi sono reso conto della distanza esistente fra l'Europa, l'Italia in modo particolare, e gli Stati Uniti riguardo alla diffusione dell'uso della telematica. Il primo problema, quindi, non è stato quello di proteggere i minori dalla rete ma di attrezzarli affinché potessero avervi accesso, nell'ottica del diritto all'informazione in rete visto come un aspetto del diritto degli stessi minori a crescere.

Inoltre era necessario far conoscere cosa si potesse fare con le macchine, evitando di usare passivamente *software* e di ricercare soluzioni preconfezionate: come diceva prima l'ingegner Nuti, lo scopo era consentire ai giovani di orientarsi. Secondo me l'Europa – come ha già cominciato a fare – dovrebbe sostenere maggiormente la causa dell'*open source*, vale a dire quel *software* gratuito, elaborato nelle università, che permette ai ragazzi di esprimersi e di essere creativi nella rete. Il pericolo non è dato dalla pornografia ma dalla stupidità della rete,

da casi come quello di Microsoft che acquisisce informazioni su quello che i nostri ragazzi fanno, sui loro gusti, sulle loro preferenze, per bombardarli con la sua pubblicità.

La difesa che dovevamo approntare non era rivolta ai contenuti pedopornografici ma – lo ripeto – alla stupidità: questo è il più grosso pericolo della rete.

In secondo luogo, viene in considerazione il problema della violenza come modalità di porsi in rete, quindi della possibile prevaricazione del più forte sul più debole, che va contro lo spirito della stessa rete. Su Internet si cerca di creare una comunità di persone che collaborano, che si aiutano, che sviluppano insieme soluzioni ai problemi. La rete non è solo un modo di comunicare: è un modo di essere, di vivere i rapporti con gli altri; è un vero luogo democratico in cui ciascuno ha la possibilità di esprimersi. Tutto questo non va compresso né mercantilizzato: va invece sviluppato. Nelle nostre scuole il *software* preconfezionato dovrebbe essere proibito e gli alunni dovrebbero poter utilizzare programmi sviluppati dagli stessi studenti.

Per quanto riguarda la protezione dei minori dai contenuti con un impatto emotivo troppo forte (a volte sono gli stessi adulti che restano sorpresi da certi contenuti della rete), non è pensabile ricorrere a una sorta di *imprimatur*, come potrebbero essere i PICS, analogo a quello che la Chiesa metteva una volta sui libri che si potevano leggere negandolo agli altri. I PICS vogliono essere una sorta di *imprimatur* sulle pagine attendibili della rete. Abbiamo visto che questi strumenti falliscono, per le ragioni prima accennate.

Anche i *software* installati sulle macchine presentano due inconvenienti: in primo luogo, sono a pagamento, e sono cari; in secondo luogo, non sono sempre aggiornati ed hanno difficoltà ad essere installati. Dopo aver sperimentato i vari *software* di protezione abbiamo deciso di creare un filtro in rete, non basato su parole chiave (se ad esempio si esclude la parola *sex* non potranno essere visualizzati tutti i contenuti in cui questa parola è usata in modo positivo: vietare un contenuto in base alla presenza di una parola non è logico né intelligente), ma su un'analisi dei contenuti, suddividendoli per categorie. Esistono reti commerciali negli Stati Uniti che già procedono da anni in questo senso, mentre non ne esisteva nessuna in Italia ed in Europa.

Attualmente sono circa un migliaio i volontari che lavorano per la rete italiana di tutela dei minori; è un enorme patrimonio rappresentato dalle persone che quotidianamente osservano quanto viene pubblicato in rete: se vi sono contenuti ad impatto troppo forte per i minori (nella categoria della violenza, in quella delle pornografia o ancora in quella dell'occultismo, che sono le tre categorie che filtriamo maggiormente in Davide.it) essi vengono esclusi nel giro di pochi minuti. Se vi sono contenuti illegali, vengono segnalati contemporaneamente alla polizia informatica; tuttavia dall'11 settembre quest'ultima riceve le segnalazioni ma non gli dà seguito, perché attualmente le sue ricerche sulla rete sono rivolte altrove. A settembre abbiamo denunciato un sito pedopornografico che ha sede in Olanda: abbiamo individuato esattamente la strada ed il numero civico in cui si trovava un *computer* che chiedeva ai ragazzi italiani ed europei di mandare autoscatti erotici in cambio di una ricarica del cellulare. Tutto avviene all'interno delle mura domestiche: un autoscatto con la macchinetta digitale, un invio del *file* del formato richiesto e si ottiene la ricarica del cellulare.

Di fronte alla pericolosità di materiali come questo presenti nella rete si sporge denuncia all'autorità di polizia che peraltro – per le ragioni dette prima – non ha la possibilità di intervenire, soprattutto se il *server* non risiede sul territorio della nostra Repubblica.

Per quanto riguarda poi i contenuti che possono essere prodotti dai ragazzi, abbiamo la possibilità di monitorare ciò che essi pubblicano su Internet: non solo le pagine da scaricare, quindi, ma anche quelle che producono. Per questo abbiamo proposto, insieme con alcune scuole, un lavoro di misurazione dell'*output* e del-

l'*input* su
Internet: si analizza, ad esempio,
la quantità di *file* musicali o di una determinata categoria scientifica, per verificare la produzione relativa di queste stesse classi rispetto a tali argomenti. Si può fornire agli insegnanti ed agli educatori in genere uno strumento di analisi della navigazione complessiva degli studenti, così da consentire loro di controllare quali tipi di *file* i ragazzi guardino. Si tratta di un'analisi utile per la didattica, che permette anche di valutare la qualità e la quantità dei documenti pubblicati dagli stessi studenti nei *server* messi a loro disposizione.

Posso fornirvi alcuni dati relativi a Davide: sono pochissime le famiglie che utilizzano la protezione per i ragazzi. Gli utenti di Davide sono circa 15 mila; non so quanti possa averne Virgilio, ma comunque sono molto pochi. È anche vero che esistono altri strumenti di controllo e soprattutto – come si diceva prima – la presenza dei genitori. Il filtro non è necessario se vi sono genitori attenti e non è sufficiente nel senso che può filtrare il 97 per cento dei contenuti, ma il restante 3 per cento non può essere controllato. Sul sito della polizia si può leggere un bel decalogo dei comportamenti che i genitori dovrebbero seguire rispetto alla rete: diffondere i contenuti del sito della polizia di Stato affinché i genitori li conoscano sarebbe assai importante.

Alcuni ragazzi ci hanno chiesto in prima persona l'attivazione del filtro. I genitori a volte non sanno impostare il *software* oppure lo usano in modo improprio: i figli vogliono essere tutelati anche dai genitori che usano impropriamente il *computer* per ricercare materiali che i primi non desiderano avere sul proprio PC.

Questa è l'esperienza di Davide.it. Dal punto di vista dei contenuti del filtro, c'è una bella rete di aggiornamento che quotidianamente rende il filtro stesso efficace. La gratuità che abbiamo voluto riservare a questo servizio per poter raggiungere il maggior numero di ragazzi ci ha però portato ad una situazione economica di grave perdita, data la mancanza di sensibilità da parte dell'opinione pubblica rispetto al lavoro che si sta svolgendo.

MATTEO FICI, *Presidente dell'Assoprovider*. Vorrei aggiungere due osservazioni: la prima riguarda Davide.it, la seconda un progetto da me presentato a suo tempo per la tutela dei minori su Internet.

Sono palermitano e tre anni fa, rispondendo al bando del comune di Palermo che si richiamava alla legge n. 285 del 1997, concernente interventi in favore dei minori, ho presentato un progetto che consisteva nel trasformare in una sala informatica un autobus fra i tanti che l'azienda municipalizzata non usava più per portarlo in giro per la città. Doveva fermarsi nei vari quartieri, nelle parrocchie, nelle delegazioni, per un paio di giorni: pensate che si trattava di un autobus molto colorato, che richiamava l'attenzione, e nel quale si svolgevano una sorta di « corsetti » di informatica in cui, in mezza giornata, si spiegava cosa fosse Internet e come si potesse adoperarlo in modo sicuro.

Il progetto avrebbe avuto un costo risibile: si poteva utilizzare il personale delle associazioni, gli autobus già esistevano, i *computer* che giravano erano sempre gli stessi; ciononostante, esso è stato bocciato, definendolo letteralmente « eccessivamente innovativo ». Sono passati circa 300 progetti: mi è stato detto che Palermo è una zona di confine ed esistono problemi molto più gravi, che non si sapeva quante persone avessero il *computer* a casa e che non era possibile misurare l'impatto del mio progetto. Ho risposto: fate 299 progetti di pronto intervento, ma almeno uno di carattere innovativo (visto che la legge riguarda proprio interventi innovativi) accettatelo ! Non è stato possibile: si è detto che il progetto era buono, che rientrava perfettamente in tutti i parametri, ma che – dal momento che non era possibile quantificare il suo impatto sul territorio – non era possibile finanziarlo.

A don Ilario Rolle è accaduto di presentare un progetto, credo attinente a

Davide,
nell'ambito del programma comunitario *safe use of Internet* (creato appositamente per attuare strumenti di filtro della rete), che è stato bocciato perché definito « poco innovativo ». Ricordo che si tratta sicuramente della prima esperienza in Italia e di una delle prime in Europa.

Sto raccontando tutto questo perché i politici devono fare attenzione ai progetti attuati nell'ambito degli strumenti che già esistono: la legge n. 285 del 1997 è ancora operativa. A mio avviso, se viene elaborato qualche progetto che riguarda Internet occorrerebbe riservare ad esso un minimo di attenzione. Se a Palermo tre anni fa fosse partito il progetto dell'autobus, chiamiamolo così, che aveva il pregio di essere visibile e di muoversi, si sarebbe attuata un'alfabetizzazione capillare e le famiglie, anche se non avevano un *computer*, avrebbero saputo cos'è Internet e cos'è un filtro. Naturalmente lo stesso vale per la televisione: si deve spiegare ed informare. Certo, non si può pensare ad Internet come ad una *commodity* per i cellulari. Come ha detto giustamente l'ingegner Nuti durante un'audizione presso l'*Authority* per le comunicazioni, questo progetto è stato realizzato da un Internet *service provider*, non da un operatore telefonico. Le nostre aziende hanno una specie di ruolo sociale perché portiamo Internet nelle province, nelle parrocchie, eccetera; altrimenti, Internet diventerà come la televisione, la *baby sitter* dei ragazzini.

È necessaria, insomma, un po' di attenzione anche sugli aspetti culturali del fenomeno: se Internet viene correttamente utilizzato è uno strumento formidabile di sviluppo, soprattutto per il Mezzogiorno. Se oggi parlate con chi ha un sito *web* vi dirà che non serve a niente, che non ci passa mai nessuno, che ci sono le immagini pedopornografiche: ma queste situazioni si possono affrontare e nessuno può pensare di escludere l'Italia da Internet.

PRESIDENTE. Ringrazio i nostri ospiti anche per il fatto che ci stanno fornendo una visione del loro lavoro molto più calata nel reale di quanto potrebbe apparire alla luce del carattere negativo che i fatti di cronaca lasciano trasparire sul mondo in cui operano.

Do ora la parola ai colleghi che intendano porre domande o richieste di chiarimento.

SILVANA PISA. Condivido il punto di partenza: dobbiamo gestire il rapporto tra libertà e tutela dei minori senza essere censori; uno dei pregi maggiori della rete è proprio quello di consentire la libertà. La rete può essere anche Echelon: i livelli di indagine rispetto alla libertà dei cittadini possono essere molto sofisticati.

Condivido inoltre l'accento posto sul problema della responsabilità dei genitori: l'educazione alla libertà riguarda anche l'uso dello strumento. Si pone però anche la questione di un vostro codice deontologico, interpretato come un elemento che garantisca la qualità del vostro servizio rispetto alla concorrenza. Si parlava prima di una sorta di « bollino blu » per chi aderisce a tale codice.

Anche il problema dell'anonimato si intreccia con quello della libertà. Per la stampa c'è la figura del direttore responsabile, mentre se si distribuisce un volantino deve apparire il nome di chi lo ha stampato; un fax reca l'indicazione del numero che lo ha inviato ed anche le telefonate sono rintracciabili. Credo che la soluzione giusta sia quella dell'anonimato protetto, anche se occorre precisare meglio le modalità della sua attuazione. Il problema è trovare il modo di far sì che la moneta buona possa cacciare quella cattiva: è soprattutto una questione che interessa voi, ma accettiamo suggerimenti. Inoltre è necessario che su questo tema si elabori una proposta democratica molto partecipativa. Oggi qualsiasi centro sociale è un utente di Internet molto sofisticato. È possibile che non emerga una proposta molto partecipata di autoregolamentazione ? Certo, ci saranno opinioni diverse sul contenuto della libertà, i cui confini si giocano anche in Parlamento, ma può essere interessante che la proposta emerga a livello di base.

ANTONIO MONTAGNINO. Anch'io ritengo che non si possa fermare il pro-

gresso ma che si debba vigilare sui suoi effetti. Non si può fermare la diffusione di Internet, che equivale a formazione, informazione e così via, ma esso presenta inconvenienti. Uno di questi è che esistono consumatori di immagini pedopornografiche e produttori delle stesse. Sicuramente le due categorie non coincidono e per la seconda è un fatto di *business*.

Secondo me il problema della pornografia e della pedofilia non è riconducibile interamente a Internet. Non credo che a Palermo, all'Albergheria, avessero questi problemi: era tutta un'altra cosa. Ho raccolto dei dati sulla base delle audizioni che abbiamo svolto in questa Commissione durante la scorsa legislatura: ad ottobre del 2000 erano stati individuati 3.363 siti di pedofilia *on line*; spero che non siano aumentati. Sono dati forniti dalla polizia delle telecomunicazioni.

PAOLO NUTI, *Presidente dell'Associazione italiana Internet providers*. Non credo fossero solo siti, ma siti ed utenti insieme.

ANTONIO MONTAGNINO. Sì, certo. A quella data non risultavano siti italiani che vendessero materiale pedopornografico. Era un dato tranquillizzante e spero che la situazione oggi sia la stessa.

La polizia delle telecomunicazioni svolge una ricerca per individuare, in base alle chiamate, i consumatori delle immagini fornite dai siti pedopornografici. Si può incrementare ulteriormente un'azione che coinvolga tutte le aziende di *provider* affinché procedano esse stesse ad identificare le chiamate, agevolando così il compito della polizia delle telecomunicazioni? Che problemi implicherebbe una simile iniziativa?

È stato detto che bisogna difendersi dalla stupidità e dalla violenza. Ritengo che, al di là delle intenzioni della politica, il rischio sia di mettere in campo solo delle parole. Ho qui con me la decisione del Parlamento europeo del 25 gennaio 1999: vorrei sapere da voi che operate in concreto – in particolare nel settore della prevenzione e del controllo – se sia stato fatto effettivamente qualcosa in relazione alla creazione di una rete europea di *hot line* ed in merito alla questione dei filtri.

Non sono un esperto in materia informatica. L'ingegner Nuti ha detto che lo strumento dei filtri è scarsamente utilizzato e che è necessaria un'opera di sensibilizzazione. Non si potrebbero collocare questi filtri nei *computer* nel momento in cui vengono venduti? È importante che le famiglie seguano l'attività del minore su Internet, ma dotare i PC dei filtri all'origine sarebbe molto utile; ovviamente la questione riguarda anche i costruttori di *computer*.

Sottolineo anch'io il tema del codice di autoregolamentazione e l'opportunità di concludere accordi internazionali, il che forse rappresenta l'impresa più difficile. Se non ricordo male, durante un'audizione svolta con i rappresentanti della polizia delle telecomunicazioni si faceva presente che non sempre il sito ed il *provider* coincidono a livello mondiale. Una difficoltà della ricerca consiste proprio nell'identificazione dei soggetti: a volte si trattava di società appositamente costituite. Si diceva che il nostro paese riserva un'attenzione molto maggiore al problema della pedofilia rispetto ad altri come gli Stati Uniti o alle nazioni dell'Est europeo, dove c'è maggiore tolleranza.

AMEDEO CICCANTI. Vorrei chiedere se, invece di intervenire sugli effetti, non si possa tecnicamente aggredire a monte il fenomeno. È possibile che organismi internazionali come le Nazioni Unite possano definire – così come avviene per il terrorismo internazionale – degli accordi per limitare il fenomeno? Oggi ci rimettiamo alla tecnica come fatto spontaneo, ma il problema è politico: se esistesse un governo di queste attività tecniche la questione si potrebbe risolvere oppure ci dobbiamo rimettere allo spontaneismo della rete?

PRESIDENTE. Do ora la parola ai nostri ospiti perché rispondeano ai quesiti formulati.

ILARIO ROLLE, *Rappresentante dell'Asoprovider*. Vorrei anzitutto dire che mi

preoccupa
che la polizia corra dietro ai tre
o quattro mila pedofili o presunti tali che vanno alla ricerca di quelle immagini; il più delle volte può trattarsi di persone che sono capitate sui siti per sbaglio o per semplice curiosità. Mi preoccupa, insomma, che qualcuno pensi di profilare la navigazione degli utenti italiani per verificare cosa facciano: rientra nella sacrosanta libertà di ciascuno vedere cosa ci sia sulla rete.

Esistono esempi di paesi che hanno bloccato alcuni contenuti. Il primo è stato la Francia, che ha fermato la vendita di oggetti nazisti: quel paese ha imposto a tutti i *provider* francesi di oscurare i *link* a quelle pagine. Nel 2001 la Svizzera ha bloccato cinque siti a livello internazionale. Ciò rientra nelle facoltà dei singoli Stati, che possono imporre ai *provider* di impedire la visione di siti ritenuti illegali: tecnicamente ciò è complesso ma possibile; è stato fatto e funziona. Bisognerà naturalmente riconoscere un compenso ai *provider* per il lavoro svolto in tal senso.

ANTONIO MONTAGNINO. Don Ilario, vorrei ricordarle che l'Unione europea ha stanziato 25 milioni di euro per l'attuazione di piani d'azione.

ILARIO ROLLE, *Rappresentante dell'Assoprovider.* Si tratta di compiti che possono certamente essere assegnati ai *provider*.

Per quanto riguarda la questione di chi produce a monte i contenuti e li mette in rete, abbiamo calcolato che sono più di tre milioni i lavoratori addetti alla produzione di pornografia in rete. La polizia potrà fornire documentazione al riguardo. Sul nostro filtro sono bloccati più di tre milioni e mezzo di siti; a ciò corrispondono decine di milioni di documenti e altrettanti di immagini e di *banner* animati. Calcolando approssimativamente il numero di ore necessario per produrre quel materiale, siamo arrivati a desumere quel numero di addetti ai lavori. Esiste quindi un mercato notevole. La diffusione di un filtro che impedisca l'accesso a questi materiali comporta un danno economico notevole per una parte della rete: non bisogna dimenticarlo. C'è un paese, la Finlandia, che ha autonomamente deciso di proibire la visione della pubblicità su Internet ai bambini. Sono in corso sperimentazioni con *provider* finlandesi che consentono di vedere il contenuto del sito bloccando tale pubblicità, ritenuta illegale.

Sui nostri siti, anche quelli scolastici, compare spesso della pubblicità, non sempre a contenuto positivo: nel tentativo di sviluppare il filtro di Davide abbiamo tenuto presente questo aspetto ed abbiamo bloccato la pubblicità di alcuni *advisor* che non distinguevano tra *banner* pubblicitari adatti alla famiglia e altri con contenuti non consoni a tale pubblico.

Pensare di arrestare a monte la produzione di determinati contenuti non ha senso: Internet è lo specchio dell'umanità. C'è tutto il nostro negativo e tutto il nostro positivo: è la vita e non possiamo – permettetemi la citazione – separare il grano dalla zizzania; crescono insieme sulla rete e non possiamo uccidere quest'ultima per tentare di estirpare la zizzania.

PIERO PELLICINI. Vorrei fare ancora una domanda. Se giungo in possesso, per motivi professionali, della carta da lettera di un avvocato di Trapani o di Pavia con il quale ho contatti, la faccio stampare, scrivo qualcosa di diffamatorio sul presidente del tribunale di Forlì, per fare un esempio, e la firmo, probabilmente poi arresteranno il collega.

Ciò che mi fa paura, insomma, è che sia possibile entrare nella rete a nome di un altro e viceversa.

PAOLO NUTI, *Presidente dell'Associazione italiana Internet providers.* La ringrazio di aver posto questa domanda. Nel fare l'esempio ero convinto di riferirmi all'attualità nella misura in cui, sul giornale di ieri, ho letto che l'onorevole Tremonti ha denunciato un ignoto che a nome dello studio Tremonti faceva pubblicità offerte dallo studio legale. È chiaro che qualora qualcuno avesse risposto a questo ignoto lo studio Tremonti sarebbe

caduto dalle nuvole, e forse per questo l'onorevole Tremonti se n'è accorto.

Questo è un problema molto vecchio. Per come funziona la posta elettronica, chi manda l'*e-mail* si qualifica. Tutto ciò cambia le carte in tavola rispetto al mondo reale o no? La risposta è secondo me « no ». Mi rifaccio al suo esempio: lei viene in possesso della carta intestata del suo collega. Una falsa *e-mail* equivale in tutto e per tutto a prendere la carta intestata che lei riceve come una denuncia, metterci sopra un foglio di carta bianca, passarla nella fotocopiatrice: il risultato è una copia che non resiste ad un esame meno che superficiale. Comunque, lei ci può scrivere quello che vuole, appone una firma – anch'essa fotocopiata – e poi spedisce il tutto via fax.

PIERO PELLICINI. Allora, se ordino una cassetta pornografica...

PAOLO NUTI, *Presidente dell'Associazione italiana Internet* providers. I casi sono due: o ci mette l'indirizzo di casa sua, oppure quello del collega. Se arriva a casa del collega, quest'ultimo si trova impelagato in un grosso problema proprio a causa della legge n. 269 del 1998.

PIERO PELLICINI. Il problema è se sono un carabiniere e vengo a sapere che gli è arrivata la cassetta...

PAOLO NUTI, *Presidente dell'Associazione italiana Internet* providers. Nel caso della posta elettronica la situazione presenta una sicurezza assolutamente maggiore rispetto alla carta intestata fotocopiata. Lei, come persona vittima di un abuso di identità, farà molta fatica a dimostrare che quel pezzo di carta intestata non è suo; invece, con la posta elettronica – come dicevo prima – solo un totale inesperto può prendere per buona l'*e-mail* che arriva. Potrei citare un episodio che risale al 1995 e riguarda l'onorevole Veltroni.

Il grosso problema di Internet è quello che ho cercato di accennare poco fa e che hanno ribadito Fici e Rolle: l'alfabetizzazione. Stiamo dando strumenti nuovi a tutta la popolazione e siamo convinti che siano utili. Immaginiamo un mondo in cui l'automobile nasca dall'oggi al domani per cui, nel giro di tre anni tutti la posseggano: pensiamo a quanti morti ci sarebbero prima che tutti sappiano guidare. Come si potrebbe fare, allora? Mandando tutti a scuola guida. Questo deve essere secondo me il ruolo delle istituzioni.

Durante la scorsa legislatura sono stato portatore, tutte le volte che ne ho avuto occasione, di un'istanza che rivolgevo a chiunque mi capitasse « sotto le grinfie » fra i legislatori: quello di Internet e dei *computer* nelle scuole è un falso problema, perché i ragazzi lo sanno usare. L'alfabetizzazione informatica è una questione che riguarda il cinquantenne, che non può essere mandato a casa. C'è un problema sociale molto più grosso.

Pian piano questa esigenza si è affermata ed ho avuto una forte gratificazione quando, verso la fine della scorsa legislatura, sono stati elaborati piani di formazione nella pubblica amministrazione molto vasti. Dobbiamo far capire a tutti coloro che usano il *computer* che quando ricevono un'*e-mail*, se sanno per certo che quello è il mittente possono fare a meno di andare a guardare l'*header*, altrimenti è il caso che gli diano un'occhiata. Potranno così verificare il dominio del *server*: se io fossi un suo corrispondente abituale saprei che normalmente usa il dominio « camera.it »; se andassi a verificare potrei scoprire che il suo messaggio reca l'intestazione con il suo nome e cognome seguiti dall'estensione « @camera.it », ma il *server* che ha eseguito il servizio è « Mclink.it ». Mi verrebbe subito un dubbio e quindi potrei alzare il telefono e chiedere se sia stato lei a mandarmi quell'*e-mail*. Quindi, la soluzione esiste ed è migliore della carta intestata.

Debbo ringraziare l'onorevole Pisa per aver parlato dei codici deontologici, che dovevano rappresentare il punto centrale della parte finale della mia relazione; poiché ho cercato di abbreviare, non ne ho parlato. L'aspetto fondamentale su cui riteniamo si debba agire riguarda la crea-

zione – e in parte ciò è avvenuto – di un contesto normativo che – come si verifica per i codici deontologici dei giornalisti – dia ai codici dei *provider* un valore coattivo nei confronti degli stessi.

Il codice deontologico assume un'importanza anche maggiore della norma legislativa perché siamo di fronte ad un fenomeno in rapidissima evoluzione: oggi esistono certi servizi, fra sei mesi potrebbero essercene altri, per cui dobbiamo disporre di principi guida fissati dalla legge e di strumenti pratici per gestire gli aspetti particolari che possono essere aggiornati contemporaneamente alla tecnologia. In altri settori si è verificato che il codice deontologico è efficace; riteniamo che debba essere promosso anche nel settore dell'accesso ad Internet.

Quanto alla proposta di forte partecipazione democratica nella definizione di questi codici, ho consegnato alla Commissione il testo dei due codici di autoregolamentazione prodotti nel 1998 (e quindi sono vecchissimi, nell'ottica di Internet) dall'Associazione italiana Internet *providers* e dall'ANFOV, che non è presente in questa sede, ma di cui sono consigliere: originariamente si trattava dell'Associazione nazionale dei fornitori di videoinformazione; poi si è trasformata e attualmente si occupa della convergenza nella multimedialità.

Questo codice dell'ANFOV è, secondo me, molto più maturo di quello elaborato dall'associazione di cui sono presidente; comunque è assolutamente chiaro ai colleghi di ANFOV (e credo anche a quelli di Assoprovider) che il codice di autoregolamentazione non può che essere unico. ANFOV si sta già facendo parte diligente per l'aggiornamento del codice e AIIP aderisce a questo progetto; immagino che i colleghi di Assoprovider saranno disponibile a lavorare con noi piuttosto che da soli.

Il punto è: che intervento ci deve essere su questi codici da parte degli utenti ? Tali codici furono prodotti in una riunione a cui erano presenti tutte le parti sociali (fornitori di servizi, utenti, associazioni di categoria), oltre a rappresentanti dei Ministeri dell'interno, delle comunicazioni e della pubblica istruzione, che si tenne nel 1998 presso il Ministero delle comunicazioni. Abbiamo depositato i codici, ai fini di un loro esame, ma nessuno ci ha più detto nulla.

Oggi la situazione è diversa. C'è uno strumento normativo, la delibera che prevede espressamente che il Garante della *privacy* si attivi per chiederci i codici ed eventualmente li approvi se sono di suo gradimento. Quindi, si è fatto un passo avanti. Riteniamo di poter cogliere questa opportunità; chiaramente, nella valutazione di questi codici potrà essere previsto anche un intervento della controparte, vale a dire degli interessati. In un certo senso durante la mia esposizione ne ho parlato: dal lato « pubblico » troviamo i due opposti che ho menzionato. C'è chi ritiene che tutto ciò che avviene in rete debba essere protetto da un totale anonimato: una posizione che definirei *cyberpunk*, che è propria però anche di molti che temono che la loro *privacy* sia fortemente compromessa da strumenti su cui ho molto calcato la mano, senza tuttavia dire nulla di falso.

La possibilità di questa « dossierizzazione » globale è dietro la porta. Personalmente – lo dico come cittadino più che come fornitore di servizi – non ritengo che ciò sia accettabile.

Dall'altro lato c'è la posizione opposta: dobbiamo trovare una convergenza. Il concetto di « anonimato protetto » non è farina del mio sacco. Se vogliamo dirla tutta, ho sentito pronunciare per la prima volta questa espressione (che ho giudicato ragionevolissima) dal professor Rodotà, prima che fosse nominato Garante della *privacy*. Quindi non abbiamo inventato nulla e le proposte sono frutto della ricerca di una convergenza su questi aspetti. Dobbiamo valutare i diritti degli utenti in tutta la loro importanza e nella mia esposizione ho cercato di rappresentarli.

Il senatore Montagnino chiedeva cosa possano fare i *provider* per individuare i fornitori e credo intendesse anche i clienti della pedopornografia. Si tratta di un problema delicatissimo: i *provider* possono

fare due cose, a cominciare da ciò che già stanno facendo. Infatti, tutte le indagini di cui si ha notizia attraverso la stampa sono state portate avanti grazie all'attività dei *provider,* che hanno fatto la loro parte tenendo nota dei *log* degli accessi e dell'assegnazione temporanea dei numeri IP di cui si parlava prima. Se non fosse stato compiuto ormai da anni e sistematicamente tale lavoro, non sarebbe stato possibile condurre le indagini perché il cliente ed il fornitore godrebbero del totale anonimato.

Il passo successivo potrebbe essere quello di analizzare i comportamenti di ogni utente al fine di determinare se egli navighi su siti che forniscono materiale pedopornografico. Questo secondo passo – attenzione – corrisponde esattamente alla « dossierizzazione » totale della popolazione di cui ho parlato nella mia esposizione. Per verificare se un mio cliente sta utilizzando materiale pedopornografico devo anzitutto individuare i siti pedopornografici e quindi predisporre uno strumento che controlli se i miei clienti li stiano visitando. Il *provider* deve quindi trasformarsi in inquirente dell'attività dei suoi clienti. Personalmente, come presidente dell'associazione, ritengo che la figura giuridica del *provider* non comporti la possibilità che egli faccia l'inquirente; il *provider* deve fornire i mezzi tecnici per eseguire le intercettazioni disposte e controllate dal giudice.

A proposito dell'archivio centralizzato, non abbiamo inventato nulla: per parlare di una sede pubblica in cui è stata ventilata questa ipotesi citerò un convegno sul *cyber crime* organizzato in seno al G8 a Parigi. Si è parlato di allestire un archivio centralizzato cui le forze dell'ordine possano accedere, ovviamente con il controllo di un garante o del magistrato. Tuttavia, se analizziamo la storia, nessuno può mettere la mano sul fuoco rispetto al fatto che, qualora venga creato un archivio centralizzato unico, non si realizzino prima o poi abusi.

ILARIO ROLLE, *Rappresentante dell'Assoprovider.* Vorrei aggiungere che, se si vogliono davvero commettere crimini in rete, si cancelleranno le tracce, utilizzando tutti gli *anonimizer* possibili per evitare che la navigazione sia esaminata. Con questo sistema avremo la possibilità di analizzare la vita di tutti i navigatori « normali », ma non dei malfattori, il che non è affatto ciò che stiamo cercando di fare.

PIERO PELLICINI. Una decina di giorni fa, durante il congresso nazionale dell'organismo unitario dell'avvocatura, ho proposto che si crei una sede, possibilmente estesa anche alla partecipazione della magistratura, per la valutazione degli atti in materia penale e di procedura penale del Parlamento europeo e del Consiglio d'Europa. Credo che il problema di fondo non sia tanto il diritto penale quanto la procedura. In alcuni Stati la legislazione è diversa da quella italiana: per esempio in Olanda in materia di droga. Non possiamo pretendere che in quel paese si applichi la nostra normativa. Invece i sistemi di indagine sono comuni. Tutto ciò di cui abbiamo parlato oggi dovrebbe, secondo me, tradursi in uno sforzo dell'Europa e dei paesi anglosassoni per unificare le norme di procedura penale e di indagine (affidate rispettivamente al magistrato e alla polizia giudiziaria) e definire un sistema generale lasciando ad ogni singolo Stato un margine di autonomia: è evidente che se un certo fatto non è considerato reato in uno Stato, non si può imporre che venga valutato come tale.

La nostra Commissione, che dovrebbe fornire alle Commissioni competenti il materiale su cui lavorare, deve assumere un respiro internazionale e stabilire collegamenti in tal senso, per dare maggiore incisività alle nostre iniziative e alimentare un colloquio coi nostri *partners* europei.

Permettetemi, in conclusione, di ringraziarvi per il vostro contributo: è stato davvero un piacere ascoltarvi.

PRESIDENTE. Vorrei a mia volta ringraziare i nostri ospiti per il loro utilissimo apporto ai nostri lavori. È particolarmente importante che il nostro incontro

si sia svolto dopo quello che la Commissione ha tenuto con il ministro Stanca, nel senso che da parte vostra è venuta un'ulteriore conferma di quanto già c'era stato detto. Per quanto riguarda in particolare il codice di autoregolamentazione, qualora riusciste a definirne uno comune il ministro Stanca ha manifestato un forte interesse nei confronti del concetto di « bollino di qualità », visto anche come mezzo per garantire un ritorno in termini economici sul *provider* della certificazione di qualità. Ciò comporterebbe anche la possibilità di suscitare un maggiore interesse ad aderire al codice deontologico in tutti gli operatori.

Premesso che condivido la necessità, espressa dal senatore Pellicini, di effettuare una proiezione europea dell'operato di questa Commissione, vorremmo attivarci, in accordo con il ministro Stanca, sul fronte della pubblicizzazione del codice di autoregolamentazione e del servizio, anche attraverso *spot* che potremmo promuovere di concerto con il ministro stesso. Si deve usare in positivo il sistema di comunicazione, in particolare quello radiofonico e televisivo.

Vi ringrazio ancora una volta e credo proprio che ci avvarremo ancora del vostro lavoro, soprattutto in vista dell'elaborazione di una proposta di legge in materia di pedofilia che terrà largamente conto, per quanto riguarda gli aspetti relativi all'attività dei *provider*, della vostra esperienza, per servire meglio l'interesse del cittadino.

Dichiaro chiusa l'audizione.

**La seduta termina alle 16,20.**

*IL CONSIGLIERE CAPO DEL SERVIZIO RESOCONTI*
*ESTENSORE DEL PROCESSO VERBALE*
*DELLA CAMERA DEI DEPUTATI*

DOTT. VINCENZO ARISTA

*Licenziato per la stampa*
*il 20 febbraio 2002.*

STABILIMENTI TIPOGRAFICI CARLO COLOMBO