



# INTERNET & LA PORNOGRAFIA

Michele Crudele  
Internet & la pornografia  
New Media, Studi Cattolici 1999; pagg. 206-10  
Archivio Biblioteca del "Campus Bio-Medico"

Copia esclusivamente ad  
uso personale o di ricerca

Anche se in proporzione limitata rispetto al totale delle informazioni disponibili sulla Rete, la diffusione di siti pornografici su Internet raggiunge livelli molto alti, superiori a quanto un utente occasionale possa percepire. Oltre ai siti famosi, legati a riviste, esiste una miriade di piccoli e grandi fornitori che, gratis per una visione parziale e a pagamento per maggiori dettagli o quantità, prosperano sulla rete. A questi si aggiungono singole persone che, per esibizionismo o come avamposto di fornitori organizzati, mettono a disposizione di tutti immagini, filmati e suoni dei tipi più bestiali.

Esistono diversi modi per arrivare a questi siti, il più comune dei quali è attraverso i cosiddetti «motori di ricerca», cioè programmi utilissimi che forniscono l'elenco di «tutte» le pagine nel mondo contenenti una determinata parola o frase (per esempio, si può provare a cercare «free sex» oppure «XXX», che negli Usa indica il massimo livello di proibizione). Altri modi sono gli elenchi di siti oppure gli abbonamenti gratuiti a *mailing lists*, cioè bollettini elettronici di nuove offerte nel settore. Il «passaparola» tra ragazzi è come sempre un veicolo alternativo abbastanza efficiente. Giornalmente le opportunità aumentano a dismisura, anche per la maggior facilità di produzione di immagini e video su Internet. Anche per una persona che non ha interesse a frequentare tali siti, è possibile imbattersi in offerte indecenti quasi involontariamente, attraverso la pubblicità presente nei motori di ricerca o in

altri siti «non pericolosi». In questo caso si tratta al massimo di un'immagine, spesso non troppo esplicita, ma sufficiente ad attirare l'attenzione.

Tuttavia, a differenza della Tv, dove lo spettatore passivo può essere bersagliato improvvisamente da pornografia esplicita (nella pubblicità o in un film), su Internet è sempre necessario un atteggiamento attivo dell'utente, che deve «fare clic» per andare a consultare determinate pagine o immagini oppure per avviare un filmato<sup>1</sup>.

La necessità di un'attiva partecipazione dell'utente alla scoperta di novità, lungi dal frenare la diffusione della pornografia, finisce per incentivarla. La curiosità di andare a vedere che cosa c'è di «speciale» in quel sito, magari annunciato con parole provocanti, è solo la prima fase di una progressiva «attrazione fatale» verso quel tipo di contenuti. L'esperienza dimostra che anche persone dotate di autocontrollo possono, a poco a poco, cedere di fronte a proposte sempre più eccitanti. Una rivista ha un numero limitato di pagine, un film porno termina dopo due ore, Internet invece non finisce mai: si salta da una parte all'altra alla ricerca di emozioni sempre più forti.

## Tentativi di difesa

Come fare a proteggersi e a proteggere le persone che abbiamo intorno? Come può un genitore tutelare i propri figli, sapendo che l'adescamento dei pedofili si ser-

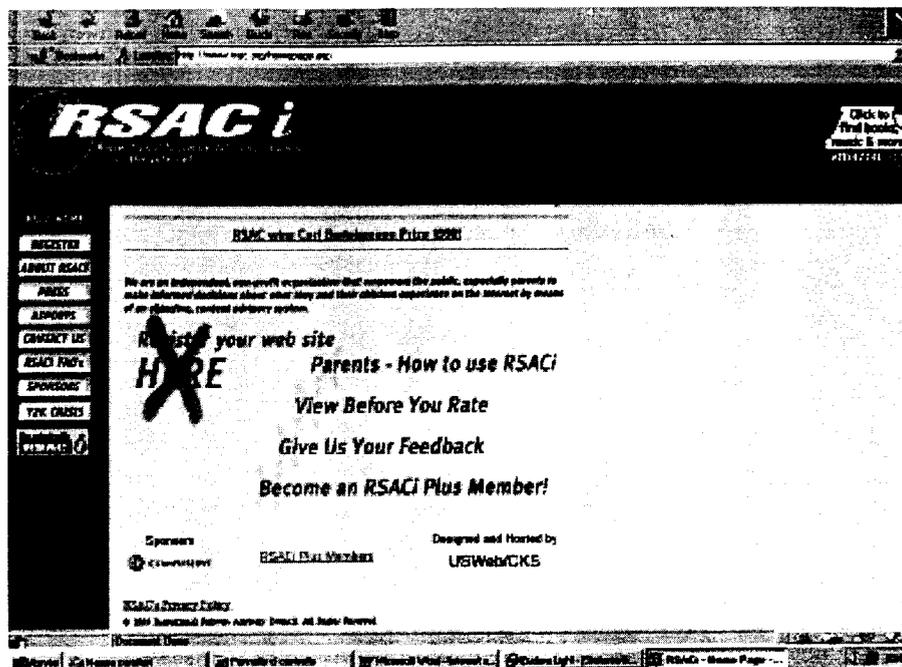
ve di questi strumenti? Non vogliamo in questa sede limitarci alla difesa dei minori, perché consideriamo la pornografia un pericolo effettivo per tutte le età, oltre che una grave offesa alla dignità umana. Con la televisione esiste un problema analogo: adottando tuttavia alcuni accorgimenti più o meno alla portata di tutti, come non vederla da soli, selezionare i programmi in anticipo, tenere in mano il telecomando per cambiare al momento opportuno, si possono evitare alcune delle nefaste conseguenze del peccato originale.

Per Internet è un po' diverso. Partendo dal presupposto che sia uno strumento di studio e di lavoro e non di mero svago (se fosse questo il caso, potrebbero essere applicati alcuni strumenti di controllo menzionati per la Tv), sembra ragionevole che in alcuni casi possa essere adoperato da soli, che richieda a volte ore di consultazione, che debba essere sempre disponibile<sup>2</sup>, che non si possano prevedere o limitare le fonti da cui attingere le informazioni. È questo il caso tipico di un'istituzione educativa di alto livello come un'università, ma può valere ragionevolmente per altre attività professionali e perfino per studenti molto giovani.

La forma più semplice di protezione è basata sul blocco (attraverso funzionalità del proprio programma di consultazione o del proprio sistema di collegamento a Internet) di tutti i siti «pericolosi». È una soluzione analoga a quella di non comprare determinate riviste o di non sintonizzare la Tv su particolari cana-

li. A parte il problema della definizione di «pericoloso», il difetto principale di questa soluzione sta nel fatto, già sottolineato in apertura, che tali siti si moltiplicano molto rapidamente. È quindi necessario aggiornare la lista di «siti proibiti» con molta frequenza. Questo compito non è alla portata del singolo, che dovrebbe dedicare ore alla settimana (se non al giorno) alla ricerca di nuovi siti da bloccare. Anche se esistono elenchi di «novità» nel settore, dai quali desumere le informazioni, si tratta pur tuttavia di un lavoro estenuante e poco produttivo.

Alcune aziende hanno percepito che poteva aprirsi un nuovo fronte commerciale e hanno iniziato, già da qualche anno, a fornire servizi al riguardo. Sono nati programmi che bloccano siti di diversa natura (pornografica, razzista, ma anche, se si vuole, sportiva, cinematografica, eccetera, con possibilità di scegliere quale categoria bloccare) e che dispongono di aggiornamenti periodici, ottenibili per abbonamento. Sono programmi da installare sul proprio computer oppure sul cosiddetto «proxy»<sup>3</sup>, come nel caso di un'azienda o di grandi centri educativi. A fronte di un costo (da alcuni considerato non irrilevante quando si tratta di centinaia di utenti), si ottiene un servizio la cui qualità è discutibile e variabile, ma che indubbiamente aiuta a risolvere il problema. Va chiarito che chi possiede la «chiave» di installazione del programma è sempre in grado di valicarne le protezioni (come colui che ha la chiave della Tv chiusa in un ar-



Questa è l'home page del sistema RSACi (*Recreational Software Advisory Council on the Internet*) che permette all'utente che impiega Microsoft Internet Explorer di visitare solamente i siti con un determinato livello di «decenza», il cosiddetto *rating*. Sono tuttavia ancora molto pochi i siti che adottano la segnalazione del proprio *rating*.

radio) con operazioni più o meno complesse. Per un utente qualunque, invece, diventa molto difficile saltare il blocco, e a volte solamente a costo della distruzione del sistema operativo.

In Italia in genere i fornitori di servizi Internet non hanno affrontato il problema e lasciano al singolo utente il compito di autodifendersi. Negli Usa esistono invece fornitori che filtrano l'accesso a Internet, garantendo ai loro clienti una navigazione abbastanza «priva di rischi»<sup>4</sup>. Sulla linea della protezione da materiale indecente, un'interessante innovazione è quella del motore di ricerca Altavista, che nella sua sezione di ricerca di immagini<sup>5</sup> permette la modalità *filtered*, cioè teoricamente priva di foto pornografiche.

## RSACi & Edunet

Esistono diversi tentativi di definire degli standard che permettano di individuare automaticamente ciò che è offensivo, osceno o violento. È un meccanismo analogo a quello dei bollini colorati

in Tv, con gli stessi vantaggi e svantaggi. Lo standard più accreditato è quello introdotto dal Platform for Internet Content Selection del World Wide Web Consortium, l'autorità che di fatto stabilisce le «regole» di Internet<sup>6</sup>. Per applicarlo, si può utilizzare il sistema RSACi (*Recreational Software Advisory Council on the Internet*)<sup>7</sup> che permette all'utente che impiega Microsoft Internet Explorer di visitare solamente i siti con un determinato livello di «decenza», il cosiddetto *rating*. Sono tuttavia ancora molto pochi i siti che adottano la segnalazione del proprio *rating*.

Esistono lodevoli iniziative italiane per affrontare il problema soprattutto per la difesa dei bambini, almeno dal punto di vista informativo, come il recente sito «Genitori & Internet»<sup>8</sup>, ma non è ancora stato prodotto un *software* nazionale completo e affidabile.

Alcune persone provenienti dalla Facoltà di Ingegneria dell'Università di Navarra, in Spagna, hanno creato nello scorso anno una società fornitrice di servizi di connessione a Internet, chiamata Edunet<sup>9</sup>, che ha un servizio di filtro per siti indecenti. È

## Utenti con connessione a Internet attraverso una rete

1. Il sito in lingua inglese [www.zdnet.com/pcmag/features/utilities98/filtering](http://www.zdnet.com/pcmag/features/utilities98/filtering) contiene un confronto delle funzionalità dei vari sistemi di filtro, includendo le caratteristiche di quelli adatti a proteggere intere reti locali, connesse a Internet attraverso *proxy*. Per esempio Cyber Patrol ha un sistema che funziona sia con Microsoft Proxy che con Netscape Proxy.
2. Un'alternativa più efficace è il software di Edunet ([www.edunet.es](http://www.edunet.es)), da installare su un sistema Microsoft Proxy 2.0 o Linux/Apache oppure Solaris/Squid. Esso si basa su una lista di siti indesiderati, aggiornata periodicamente, e sull'analisi lessicale del testo delle pagine consultate, in inglese, spagnolo, tedesco, francese, portoghese e italiano, che sono bloccate se contengono parole o frasi giudicate indecenti. L'amministratore del sistema ha alcune possibilità di configurazione per un maggior o minor rigore e per stabilire eccezioni alle regole.
3. Una soluzione a costi inferiori e con minore complessità di gestione è far passare tutte le comunicazioni Internet attraverso il *proxy* di Edunet. Questa soluzione è accettabile solamente per velocità di connessione fino a 64 Kbps e va valutata in relazione alla prevedibile diminuzione della velocità di collegamento a siti italiani di Internet, dovendo ogni transazione passare attraverso la Spagna.
4. Una soluzione differente, ma non necessariamente alternativa, è adottare un sistema di monitoraggio periodico dei siti visitati dagli utenti (soprattutto in ambienti scolastici) per verificare se l'uso di Internet è limitato alle finalità della connessione. Infatti, a volte è utilizzato anche per motivi futili o per giocare. Questo utilizzo è solo parzialmente coperto dai programmi di filtro. Risulta invece abbastanza evidente esaminando, utente per utente, che tipo di pagine ha richiesto.
5. Basandosi su un regolamento accettato e firmato dall'utente, si possono comminare sanzioni, che vanno dalla sospensione temporanea a quella definitiva dell'uso della rete, in caso di violazione. Questo deterrente si dimostra spesso molto efficace.

anche possibile usufruirne senza essere direttamente loro clienti per l'accesso a Internet. In Italia esiste da poco un referente<sup>10</sup>. Sono allo studio accordi di più ampia portata per sviluppare tale servizio anche in Italia. Recentemente il sistema di Edunet ha aggiunto alla lista di siti da bloccare anche un sistema di analisi delle parole contenute nelle pagine consultate. A tutt'oggi funziona con lo spagnolo, l'inglese, l'italiano, il tedesco e il francese.

Può capitare che pagine di contenuto positivo (per esempio un documento pontificio sulla sessualità) siano bloccate dai filtri basati su parole. Il sistema di Edunet riesce a dare un peso alle parole indecenti, lasciando perciò passare quei documenti che impiegano moderatamente la terminologia negativa. I siti pornografici, infatti, in genere non conten-

gono solamente una parola indecente, ma una sequenza di termini, oppure alcune «parole chiave». Tale sistema di analisi non è infallibile, ovviamente.

Questo approccio, che si basa sul far passare tutta la propria comunicazione Internet attraverso il *proxy* di Edunet (ora collocato in Spagna), consente una relativa tranquillità per colui che si collega da casa propria. Per un'istituzione che ha una connessione permanente a Internet può essere più conveniente installare il software di Edunet sul proprio *proxy*.

Il sistema di Edunet è più efficace di molti programmi commerciali, sia per la metodologia adoperata che per le dichiarate intenzioni educative (e non solamente economiche) dell'azienda. Ha un costo paragonabile agli altri sistemi. Il basso numero di lin-

gue può essere visto come un limite, perché in giapponese e nelle lingue slave, tanto per fare un esempio, ci sono numerose offerte pornografiche: tuttavia non è frequente che un italiano conosca i termini da cercare e inoltre l'elenco dei siti da bloccare, continuamente accresciuto, costituisce un primo bastione invalicabile. Il passaggio attraverso il *proxy* spagnolo può rallentare la navigazione, in relazione soprattutto alla velocità del collegamento Italia-Spagna, variabile a seconda del fornitore di servizi scelto in Italia. Le esperienze fatte finora non mostrano una penalizzazione evidente. Non tutto viene bloccato: per esempio i servizi *ftp*<sup>11</sup> non sono analizzati nel loro contenuto e quindi è teoricamente possibile, conoscendo esattamente le fonti, scaricare immagini e filmati da siti indecenti e poi visionarli successivamente. Tuttavia l'elenco di «siti proibiti» include molti *ftp sites* e spesso il nome del sito contiene parole oscene che sono opportunamente bloccate. Inoltre, frequentemente si parte da una pagina Internet che ricade sotto il filtro completo. Stessa cosa si può dire dei sistemi di visione di filmati<sup>12</sup>, pubblicizzati attraverso pagine Internet. Non sono invece controllati automaticamente gli allegati di posta elettronica, che possono essere immagini o filmati, e neppure i *newsgroups* (gruppi di discussione su qualsiasi tema, e quindi anche su argomenti scabrosi), quando si utilizza il protocollo *nntp*<sup>13</sup> e non le semplici pagine Internet. In futuro sarà certamente ampliata la gamma di possibilità di blocco. Nel caso di utilizzo del software sul proprio *proxy* è possibile configurare diversi livelli di severità a seconda delle necessità.

## Un filtro nel proxy

È comunque chiaro che i sistemi disponibili sul mercato, incluso Edunet, non risolvono completa-

## Protezione di un computer collegato a Internet via modem

mente il problema. È necessario un approccio più globale, soprattutto per le istituzioni educative. Si deve distinguere la situazione della singola famiglia che ha un computer collegato saltuariamente a Internet da quella dell'università, scuola o residenza di studenti che ha una rete di calcolatori connessi in modo permanente, o per lo meno frequente, a Internet.

Nel caso del singolo o della famiglia, la soluzione Edunet o di un programma commerciale può essere l'unica strada percorribile. Ne esiste una più sicura, per dare la massima protezione ai bambini, che consiste nello scegliere la soluzione inversa rispetto al blocco: consentire l'accesso solamente a una lista di siti «garantiti», magari fidandosi del già citato RSACi. Tale approccio è un po' contrario alla logica di Internet, come interconnessione potenzialmente illimitata di fonti, ma può essere più che sufficiente per fornire le informazioni necessarie a una famiglia.

Nel caso di un'istituzione, la scelta di installare un filtro a livello del proprio *proxy* sembra necessaria. Tutti i sistemi hanno la possibilità di definire una lista di siti non desiderati, che deve però essere aggiornata continuamente. È questa la protezione minima. Per aumentare il livello di sicurezza si possono scegliere programmi commerciali oppure il software di Edunet o, se le prestazioni non ne vengono a soffrire molto, il più economico accesso attraverso il loro sito.

Esiste però un ulteriore strumento che è sempre disponibile quando si lavora attraverso i *proxy*: la registrazione di tutte le operazioni effettuate su Internet. Configurando opportunamente la rete interna e disponendo di apposito software, è possibile anche monitorare le operazioni del singolo utente, tenendo traccia di chi si è connesso. Il monitoraggio consente di valutare l'opportunità e la correttezza d'impiego di Internet da parte degli utenti. In

1. Un genitore che ha il collegamento a Internet può utilizzare alcuni software relativamente poco costosi (intorno ai 50 Euro) per proteggere la navigazione propria e dei propri figli.

2. I programmi di filtro della navigazione si installano facilmente e possono essere disattivati solamente conoscendo una parola chiave. Il genitore può perciò impedire a chiunque (meno che a sé stesso) l'accesso a siti inopportuni.

3. Una lista di programmi di questo tipo è disponibile su [www.netparents.org](http://www.netparents.org), che contiene anche altri suggerimenti in inglese sull'uso di Internet da parte dei bambini. Un'altra lista abbastanza completa è in [www.worldvillage.com/wv/school/html/control.htm](http://www.worldvillage.com/wv/school/html/control.htm)

4. Un confronto delle funzionalità dei vari sistemi è disponibile, in lingua inglese, su [www.zdnet.com/pcmag/features/utilities98/filtering](http://www.zdnet.com/pcmag/features/utilities98/filtering)

5. In inglese il problema è parte del cosiddetto *parental control* (controllo da parte di genitori). I programmi fanno parte della categoria dei *blocking* oppure *filtering* software.

6. Sono in genere programmi realizzati negli Usa e perciò più accurati nel bloccare fonti in lingua inglese o del mondo anglosassone. A volte lasciano passare siti italiani pornografici, ma è possibile segnalarli e provvedono ad aggiungerli alla lista. SurfWatch e Cyber Patrol sono fra i più conosciuti. Cyber Snoop è considerato il più versatile. Di molti è possibile scaricare una versione dimostrativa che scade dopo qualche settimana. Può essere conveniente provarli per valutarne l'efficacia.

7. Il problema principale è l'aggiornamento della lista di siti non desiderati. Se non è frequente e non è ampia (inclusi quelli italiani), il software è poco efficace dopo qualche settimana. Prima dell'acquisto vanno perciò verificate queste condizioni, attraverso una lettura attenta delle caratteristiche della versione più recente.

8. Attraverso questi programmi è anche possibile agire al contrario, abilitando la navigazione solamente ad alcuni siti conosciuti e sicuri. Per esempio Cyber Patrol offre la lista CyberYES di siti divertenti ed educativi per bambini. L'utente può man mano aggiungere altri siti ritenuti interessanti. È questa la forma più sicura di approccio a Internet, anche se penalizza la capacità di espansione della base di conoscenze (chi naviga troverà spesso collegamenti bloccati).

9. L'acquisto di un programma di questo tipo prevede un aggiornamento periodico, anche molto frequente, che può essere automatizzato. Il costo annuale è dell'ordine del prezzo di acquisto iniziale.

10. La sicurezza che i propri figli non violino le protezioni è basata normalmente sulla *password*, parola chiave da inserire al momento dell'installazione: non deve essere banale. Un ragazzo molto abile potrebbe anche, con operazioni complesse, aggirare l'ostacolo, ma con conseguenze in genere visibili su altri programmi installati o con seri danni sul sistema operativo.

11. Un'alternativa più efficiente dal punto di vista della sicurezza del blocco è abbonarsi al servizio di Edunet ([www.edunet.es](http://www.edunet.es)) che dà la possibilità di far passare tutte le proprie richieste Internet attraverso un sistema di filtro centralizzato, basato sia su liste di siti indesiderati che su parole contenute nelle pagine richieste. Il sistema funziona attualmente per l'inglese, lo spagnolo, il francese, l'italiano e il tedesco, limitatamente al protocollo http (cioè le pagine abituali visibili sul WWW). Per abbonarsi dall'Italia ci si può rivolgere al sig. Marco Nicchi (email: [m.nicchi@elis.org](mailto:m.nicchi@elis.org); tel. 06.43.56.03.07 in orari di ufficio). I costi sono intorno ai 130 Euro per l'abbonamento annuale. Il sistema comporta l'installazione di un software sul proprio computer per garantire che la configurazione del *browser* di navigazione (Netscape o Microsoft) non possa essere alterata per saltare il filtro.

molte istituzioni, così come in molte aziende, l'uso di Internet è consentito esclusivamente per fini didattici e di lavoro, non per intrattenimento. L'abuso è represso, a volte anche severamente<sup>14</sup>.

Sapere di essere controllati costituisce per molti un freno nell'accedere a siti dei quali normalmente ci si vergogna. Nel caso di chi (uno studente non particolarmente formato, per esempio) non ha chiara consapevolezza dei danni che provoca la pornografia e quindi non si preoccupa che gli altri vedano il suo comportamento, può valere invece il deterrente delle sanzioni per la violazione dei regolamenti. La penalità più efficace risulta spesso la privazione temporanea dell'accesso a Internet<sup>15</sup>. Per i recidivi la sospensione definitiva risolve il problema alla radice.

## Regole per l'accesso

La verifica dei siti richiesti da un utente richiede purtroppo tempo e una buona conoscenza del mondo Internet da parte del «controllore». Possono essere, infatti, centinaia in un giorno per un solo utente. L'esperienza insegna però che l'interessato a siti pornografici non ci capita una sola volta accontentandosi di quello che ha visto: è invece un navigatore curioso, abbastanza facilmente individuabile dalla tipologia di siti consultati, anche se questi non hanno un nome<sup>16</sup>. Inoltre, poiché la funzione del controllo è soprattutto un deterrente, non sarà abitualmente necessario scandagliare in modo completo tutti gli utenti: basterà andare a campione. In questi casi sembra necessario divulgare la sanzione, affinché questa serva da monito agli altri. Può esserci qualche problema di delicatezza nei confronti del colpevole, ma poiché la sanzione è visibile (non può più usare Internet) il problema è puramente teorico<sup>17</sup>.

Diverse persone obiettano che tale metodologia di controllo è lesiva della *privacy* e non tutela la libertà. D'altra parte in un Paese notoriamente libertario come gli Usa ci sono aziende che controllano, in piena legalità, perfino la posta elettronica dei dipendenti, per evitare fughe di notizie aziendali strategiche o di software prodotto internamente.

Se si definiscono bene le regole, includendo il monitoraggio, al momento in cui si concede l'accesso a Internet a un utente, questi problemi si risolvono. Se l'utente non le accetta, non accede a Internet. Non essendo un diritto naturale, né normalmente una necessità assoluta, una simile preclusione non comporta particolari conseguenze. Il criterio è «stare alle regole del gioco», come d'altronde avviene in una qualsiasi istituzione educativa, dove l'introduzione di riviste pornografiche è normalmente sanzionata. In conclusione, posto che non esiste un sistema perfetto per arginare la pornografia su Internet, per un'istituzione educativa o per centri con più computer collegati a Internet contemporaneamente sembra necessario adottare entrambi i sistemi sopra citati: il blocco dei siti (attraverso liste aggiornate e programmi di filtro appositi) e il controllo dell'attività degli utenti.

### Michele Crudele

<sup>1</sup> Fanno eccezione i cosiddetti «canali» (tecnologia *push*) che assomigliano più a Tv a richiesta che a siti Internet. Ci si abbona a un servizio che trasmette automaticamente le informazioni con la periodicità richiesta. Alcuni esempi: risultati sportivi, ultime notizie, agenzie di stampa. I dati sono trasmessi sfruttando i tempi morti della propria connessione a Internet e sono memorizzati sul proprio Pc. Alcuni sistemi prevedono di mostrare le informazioni scaricate sullo sfondo (*desktop*) o come salvaschermo. I «canali» possono ben prestarsi agli scopi di malintenzionati, anche se non sono molto utilizzati in Italia. Il dover attivare un abbonamento a un «canale» (gratuito o a pagamento) è però condizione indispensabile.

<sup>2</sup> Non ci poniamo in questa circostanza il problema dei costi di connessione: la

valutazione costi-benefici è compito dell'utilizzatore.

<sup>3</sup> Un *proxy*, che vuol dire procuratore, è un computer che intercetta tutta la comunicazione da e verso Internet, facendo quindi da collo di bottiglia. Può avere funzioni di protezione per la rete di un'istituzione, per evitare che da fuori si possa accedere alle risorse interne. Può anche accelerare la comunicazione con i siti molto lontani, mantenendo *in loco* una collezione di pagine di frequente consultazione (la cosiddetta *cache*).

<sup>4</sup> Alcuni rischi restano sempre, sia perché i criteri di tali fornitori possono differire da quelli del cliente, sia perché è oggettivamente difficile bloccare tutto ciò che è negativo. Riguardo ai criteri di scelta, si può citare il recente episodio della pubblicazione su Internet degli atti dell'inchiesta sul Presidente degli Stati Uniti Bill Clinton, in relazione alle sue attività «improprie». Alcune società si sono rifiutate di bloccare l'accesso perché notizie già diffuse dalla stampa e dichiarate di pubblico interesse dal Congresso statunitense. Tuttavia danno la possibilità di personalizzare il proprio software aggiungendo quel sito nella lista personale di documenti proibiti.

<sup>5</sup> Altavista Photo Finder <http://image.altavista.com>

<sup>6</sup> <http://www.w3.org/PICS/>

<sup>7</sup> <http://www.rsac.org>

<sup>8</sup> <http://www.keycomm.it/geninternet>

<sup>9</sup> <http://www.edunet.es>

<sup>10</sup> Marco Nicchi (m.nicchi@elis.org): tel. 06.43.56.03.07 in orari di ufficio.

<sup>11</sup> Il protocollo adoperato per trasferire files.

<sup>12</sup> RealVideo e NetShow, soprattutto.

<sup>13</sup> Questo protocollo può anche essere inibito nelle organizzazioni che dispongono di un proprio *proxy*.

<sup>14</sup> Ci sono state persone licenziate da grandi aziende multinazionali per aver semplicemente scaricato musica da Internet.

<sup>15</sup> Se l'accesso alla rete informatica è protetto da un sistema di autenticazione (è cioè necessario inserire il proprio nome e la *password*), è possibile interdire l'accesso a Internet a singoli utenti, lasciando gli altri liberi di «navigare».

<sup>16</sup> Alcuni siti pornografici, per rendere più difficile l'intercettazione da parte di sistemi basati su filtro di parole, usano solamente il cosiddetto «numero IP», cioè l'identificativo univoco.

<sup>17</sup> Data la finalità educativa di queste sanzioni, il rapporto con il colpevole può essere gestito a vari livelli. È compito dell'istituzione definire le modalità di comunicazione (attraverso un tutore, un direttore, un amico, eccetera).