ALCUNI ASPETTI RELATIVI ALLA SICUREZZA DELL'ACCESSO A INTERNET

[1]D. De Jaco, [2]M. Guastavigna
[1] CSI-Piemonte
Corso Unione Sovietica, 216 – 10134 Torino
dario.dejaco@csi.it
[2] I.I.S. Beccari Torino
Via Paganini 52 – 10154 Torino
guastavigna@inwind.it

Riassunto

In Piemonte è stata avviata una rete per l'interconnessione di tutte le scuole. La rete ha lo scopo di favorire l'interscambio tra funzioni istituzionali ma anche un uso didattico (in senso lato) delle risorse informative disponibili. In questo quadro, le protezioni per il controllo degli accessi a siti non "didattici" sono uno dei punti più rilevanti a garanzia degli alunni (tenendo anche conto della minore età) e della responsabilità che si assumono gli insegnanti. Sono qui elencati e discussi alcuni approcci possibili al problema, con una breve descrizione di quanto messo in atto finora, ed una proposta di lavoro.

1. Cosa intendiamo qui per sicurezza

Non ci occupiamo, in questo intervento, di e-commerce, di firma elettronica, di transazioni economiche, di antivirus, di crittografia, né dal punto di vista tecnico né dal punto di vista giuridico ma solo di strumenti che servono a evitare incontri (anche casuali) tra persone con strumenti di difesa limitati e proposte troppo forti sul piano emotivo. Non affrontiamo, infine, il problema della pedofilia o degli adescamenti, in senso stretto.

2. Gli approcci attualmente in uso

Anche la navigazione "materiale" ha sempre avuto e ha i suoi rischi. Non per questo gli adulti hanno rinunciato o rinunciano a far viaggiare per mare le nuove generazioni: adottano per esse particolari precauzioni, da giubbotti di salvataggio su misura, alla costruzione di ambienti protetti per le lunghe percorrenze, all'interdizione ai bambini di certe zone della nave, contenenti dispositivi, macchinari e quant'altro possa comportare pericolo. Insomma, hanno esercitato il loro diritto-dovere di tutela.
Per la tutela dei bambini nella navigazione "immateriale", accanto a soluzioni molto sofisticate e impegnative, che prevedono l'impiego di dispositivi hardware e software complessi, esistono - nati in genere per essere usati dai genitori, in situazione domestica - numerosi strumenti di uso semplice e tutto sommato efficace che possono interessare quindi anche la scuola.
Tra questi si collocano i browser (strumenti di navigazione) per bambini. Ne è consultabile un elenco abbastanza ampio in Kids Freeware - Free Software and Internet Services for Kids.
Questi programmi prevedono un meccanismo di supervisione adulta, secondo modelli

parzialmente diversi, di cui illustriamo qui di seguito tre esempi paradigmatici:

- *Bounce* consente di generare una lista di siti sempre accessibili e simmetricamente una lista di siti mai raggiungibili; di definire un tempo massimo di navigazione giornaliero; di avere un elenco dei siti giornalmente visitati dai bambini; di utilizzare filtri per la connessione che escludono le pagine che contengono certi termini e espressioni; ciascuna di queste funzioni, inoltre, è associabile a un profilo utente diverso, con il suo login e la sua password; il programma, infine, può essere posto in autoesecuzione all'avvio di Windows e interviene a richiedere la "parental password" a ogni esecuzione di un browser tradizionale emettendo, a casse accese, un barrito di cui perfino Go!Zilla può ben essere invidioso.

- *At Kids Browser* consente anche interventi più decisi, sempre attraverso il meccanismo della supervisione adulta. È infatti possibile eliminare la possibilità di inserire indirizzi e il menu Go, per cui l'utente potrà navigare soltanto nell'ambito del bacino di siti predefinito dal genitore o dall'insegnante.

- *Childbrow* propone la soluzione più radicale: la possibilità di navigare esclusivamente nel bacino di siti definito dal supervisore adulto. A differenza dei due prodotti precedenti (shareware) è free: per poterlo usare dobbiamo soltanto al primo avvio inviare la nostra mail al centro di registrazione.

Un altro approccio, molto più restrittivo e molto discutibile, è quello proposto da RETEPULITA.IT che propone un filtro particolare (a pagamento) fatto da un operatore umano che intercetta le richieste alla rete e che le filtra (on the fly) decidendo – a suo giudizio - sull'opportunità di fornire la risposta.
Un cenno particolare a www.davide.it, il provider che offre una connessione protetta, garantendo una navigazione filtrata, veloce e sicura. I bambini non corrono così il pericolo di fare spiacevoli incontri ma, come recita l'avviso nella home page, "la navigazione dei bambini non deve essere mai lasciata totalmente in mano ai bambini, ci deve essere sempre la guida di un genitore o di un adulto in generale".
Infine c'è chi propone (non solo in Italia) un approccio secondo il quale la sicurezza parte dagli utenti finali (i bambini) e dalla loro consapevolezza sui problemi che – per strada e su Internet - possono essere chiamati ad affrontare. Quest'approccio si traduce in una serie di regole (molto ben spiegate nel caso di Tommasone Cybercop) attraverso le quali coinvolgere e responsabilizzare i protagonisti dell'evento, cioè i bambini stessi.

3. Una proposta di discussione

L'idea di interdire (in qualche modo di censurare) non è mai del tutto convincente e piacevole. Proponiamo perciò di considerare la faccenda da un altro punto di vista.

Definire un bacino di siti "consentiti" può in realtà essere per gli adulti occasione di ricerca "mirata" e di costruzione di un progetto di consultazione di informazioni secondo un senso e uno scopo utili sul piano formativo ai bambini per qualcosa di più della navigazione in sé e per sé.

Questo potrebbe dare un ruolo forte all'insegnante come guida alla "scoperta" ed alla classificazione, coinvolgendo contemporaneamente i ragazzi in un'operazione in cui non sono "sorvegliati" ma protagonisti.
Non si dimentichi inoltre che nessun insieme di siti è definitivo e esclusivo; da una parte il

lavoro può quindi essere considerato in prospettiva dinamica e dall'altra la definizione di insiemi diversi può tradursi in utili classificazioni e ordinamenti delle risorse di Internet.

4. La rete piemontese

La RUPAR piemontese (soprattutto per la parte dedicata alle Scuole) vuole e deve essere una rete sicura, protetta con una serie di meccanismi che garantiscano agli utenti, per quanto tecnicamente possibile ad oggi, il massimo grado di riservatezza da intrusioni esterne e da attività interne "non gradite".
La sicurezza è garantita dai seguenti punti di forza:

- È una sorta di Rete "privata" a tutti gli effetti, cioè chiusa e controllata, con punti di ingresso/uscita e nomi predefiniti e costantemente verificati.
- L'autenticazione è garantita da appositi Certificati digitali, che sono consegnati esplicitamente ad ogni singolo utente insieme al suo CIP (Codice di Identificazione Personale). L'insieme Certificato digitale e CIP garantisce l'identificazione dell'utente, della sua Posta e di ogni operazione che compierà in rete. Starà all'utente, naturalmente, evitare una diffusione non controllata della sua chiave di accesso.
- L'utente è autenticato ad ogni ingresso nella RUPAR e tutte le operazioni che compie vengono "tracciate" (questo avviene con il suo esplicito consenso in proposito). Il tracciamento consiste nella registrazione automatica di quanto l'utente richiede alla rete, sia pur nella garanzia dei diritti di privacy. Questa cautela serve per poter ricostruire, se servisse, eventuali comportamenti non consoni alla sicurezza dell'ambiente.
- È presente un Filtro Web (SmartFilter) che impedisce la connessione a siti classificati indesiderabili.

Ulteriori informazioni sono reperibili su http://www.scuole.piemonte.it

Il filtro in uso (che ha tutti i limiti dei filtri) è un sistema automatico che limita l'accesso ad Internet, escludendo la possibilità di collegarsi a siti Web di contenuto non desiderato. Con questo sistema la RUPAR è in grado di impedire che il personale di una scuola o i suoi allievi utilizzino la rete Internet per visitare siti non pertinenti.
È effettuata, per questo, una continua ricerca automatica, nello spazio Internet, di nuovi siti e pagine che corrispondono ai criteri di appartenenza a 30 differenti categorie predefinite in una "lista di controllo", che comprendono una vasta gamma di contenuti diversi.
Ogni nuovo sito rilevato viene verificato da una équipe di tecnici (umani) per un'analisi specifica, che serve a decidere se il sito osservato debba essere inserito in una delle categorie filtrate oppure no.
Nel vasto contesto delle norme e delle preferenze individuali, il discernimento tra contenuti leciti e non può essere oggetto di discussione. Il filtro considera i siti contenuti nelle 30 categorie suddette come improduttivi per la grande maggioranza degli impiegati e/o studenti nell'adempimento delle normali funzioni loro attribuite durante l'orario di lavoro/lezione.
Benché l'identificazione di un sito al fine della sua inclusione in una delle categorie sia il risultato di una continua analisi e ricerca, data l'evoluzione tumultuosa delle offerte in rete non è possibile garantire l'indicizzazione di *tutti* i potenziali siti appartenenti ad una determinata categoria.
Inoltre, poiché l'identificazione di un sito specifico come appartenente ad una categoria determinata potrebbe comportare problemi di corretta interpretazione del suo contenuto, la lista

non può comprendere siti che solo un particolare utente potrebbe desiderare di filtrare, ma si attiene a criteri più diffusi e generalizzati.
Infine, in una logica che prevede la massima libertà di comportamento (e di responsabilità personale), si è deciso di non filtrare nella RUPAR tutte le categorie previste dal sistema originale ma solo quelle evidentemente "improduttive", poiché la ricerca e la navigazione libera possono essere interessanti, stimolanti ed utili anche quando portano ad offerte informative più consone al gioco che allo studio in senso stretto.
Senza addentrarci negli aspetti didattici e pedagogici, l'impostazione che abbiamo dato al filtraggio serve a garantire l'utenza più esposta da pericolosi traumi ma contemporaneamente non vuole deprivarla, azzerandone i meccanismi di curiosità o nascondendo (inutilmente) il mondo reale.
Per questo si è deciso di filtrare le categorie di siti etichettate come: Comportamenti criminali, Occultismo, Appuntamenti e incontri, Droghe, Estremo/Oscenità/Violenza, Spazi per adulti, Giochi d'azzardo, Sesso. Per quanto riguarda quest'ultima categoria, va notato che, facendo riferimento alle influenze culturali e ai gusti personali, ciò che viene considerato sesso o pornografia o semplicemente una forma di divertimento può essere oggetto di dibattito, ma, nello svolgimento delle normali funzioni di impiegati e studenti, si possono considerare comunque alla stregua di contenuti improduttivi.
Contestualmente si è deciso di NON filtrare le seguenti categorie: Arte e Cultura, Anonymizers/Translators, Chat, Intrattenimento, Giochi, Informazioni di tipo generale, Hate Speech (dedicata ad ogni sorta di propaganda tesa ad incoraggiare o fomentare atteggiamenti oppressivi verso uno specifico gruppo di individui, donne, minoranze, disabili ecc., compresi gli integralismi di ogni specie, ritenendo che è meglio conoscere che ignorare), Umorismo, Investimenti, Ricerca di lavoro, Stili di vita (gusti, tendenze, orientamenti; fanno parte della lista i siti gay, transgender, i club privati, i vegetariani, i naturisti ecc.), siti musicali MP3, Nudi (cioè Sculture e pittura classica, nudi fotografici, qualche immagine naturista o dettagliate illustrazioni mediche, comprese nella categoria "Nudismo"), Vendite on line, Pagine Personali, Politica e valori sociali, Portali, Salute e cura di se stessi, Sport, Viaggi, Usenet News e Webmail.
Potrebbe essere utile trovare una qualche forma di collaborazione che permetta di interscambiare esperienze, osservazioni e strumenti tra gli operatori italiani che condividono quest'approccio.