La diffusione di Internet rende sempre più critico il problema della navigazione protetta e, più in generale, delle responsabilità che scuola e famiglia hanno nei confronti dei minori in rete.

I punti di criticità che emergono sono:

- l'uso della posta elettronica;
- la navigazione sul Web;
- la partecipazione a forum o chat di discussione;
- lo spamming;
- la diffusione della netiquette;
- la necessità di adottare nelle aule e laboratori telematici delle policy condivise di utilizzo.

Oltre ad essere evidente la necessità della presenza dell'adulto (insegnante o genitore) come guida durante le sessioni, si rende indispensabile l'adozione di soluzioni che proteggano i minori che navigano sulla rete.

Uno strumento utile per agevolare la navigazione in rete ai bambini sono i ***browser appositi***.

## BROWSER PER BAMBINI E BROWSER "FAI-DA-TE": PROGETTARE LA NAVIGAZIONE

I browser per bambini sono nati come strumenti per la tutela della navigazione dei figli da parte dei genitori, e sono, ovviamente, utilizzabili anche come strumento didattico.

I "rovistatori della rete" per bambini possono sostituire tale scelta con soluzioni più sofisticate e impegnative, che prevedono l'impiego di dispositivi hardware e software complessi, mantenendo l'obiettivo di consentire ai bambini una navigazione sicura. Il meccanismo a cui tutti questi browser ricorrono è la **supervisione adulta**, che viene però esercitata sulla base di due principi logico-operativi fondamentali, molto diversi l'uno dall'altro: il principio dell'**inibizione** e il principio della **validazione**.

Il principio dell'inibizione si fonda sulla redazione delle "**black list**": il supervisore ha il compito di inserire nel browser siti che non devono essere raggiungibili; penserà il software a bloccare l'accesso.

Il principio della validazione è basato sulla redazione delle "**white list**": il supervisore deve inserire siti consentiti, o, per meglio dire - dal momento che in base al principio di funzionamento del brower saranno gli unici raggiungibili- di fatto **consigliati** al bambino.

Prima di fornire indicazioni sul software utilizzabile a tale scopo, voglio chiarire quali sono le ragioni pedagogiche e didattiche che mi fanno optare sulla seconda tipologia di "filtrazione" e, pertanto, sulla redazione di una white list.

Innanzitutto sono convinto che **proporre è meglio che censurare**, sia dal punto di vista dell'efficacia sia della relazione formativa. La modalità "white list" può tradursi facilmente nell'occasione per realizzare un **progetto** che preveda l'uso integrato delle risorse di rete in un'attività di ricerca che interessa e coinvolge il minore non solo e non tanto perché si svolge anche su Internet.

Faccio un semplice esempio: una ricerca sull'acqua potrà prevedere che i bambini navighino su siti che trattino in modo scientifico e adatto alla loro età il tema "acqua", che l'insegnante avrà precedentemente navigato e raccolto in una "lista di siti consigliati", collocata all'interno dei meccanismi di protezione fornita dal browser in uso.

Il legame tra "white list" e "navigazione su progetto" è molto importante: è necessario fornire ai ragazzi non già le pratiche tecnologiche, ma le **competenze di elaborazione cognitiva**, dalla logica di funzionamento di un sito e delle pagine web in genere, le capacità di svolgere una vera e propria ***iperlettura***. Ogni Lettore-Navigatore deve perfezionare in modo consapevole una propria strategia di comprensione, basata costantemente sulle sue capacità

associative e deduttive, di definizione e di verifica della navigazione, intesa appunto come **percorso di lettura ipertestuale**.

Al web-navigatore, di qualsivoglia età, resta il carico, l'incombenza della ricostruzione dell'insieme, ossia del senso e dei significati dei contenuti visitati. Questo processo, che si realizza attraverso informazioni di tipo testuale, ma anche mediante immagini, suoni, filmati e le relazioni tra tali "informazioni", può aver inizio in modo efficace anche in bambini della scuola dell'infanzia e primaria.

In tal senso, per affrontare in modo propedeutico le prime tappe di un cammino cognitivo così complesso, è necessario cogliere il vantaggio fornito da ambienti con un'architettura pensata per i bambini.

Ii browser per bambini offrono non solo la tutela, ma anche la semplificazione dell'interfaccia: la medesima logica operativa di fondo e le medesime funzioni di base di un browser per adulti si manifestano in tali prodotti per bambini, praticabili dentro un ambiente dalla grafica accattivante e soprattutto dotato di icone più grandi e in numero ridotto. Anche questo è un aspetto essenziale per chi voglia evitare atteggiamenti addestrativi e come tali antipedagogici, che forzino l'anticipazione di situazioni e prestazioni troppo complesse.

Rivolgiamo, finalmente, l'attenzione ai software più interessanti, tutti fondati sul principio della "white list" e, altresì, sull'interdizione dell'attivazione di eventuali collegamenti esterni da ciascuno dei siti in essa contenuti, i quali sono invece esplorabili per tutta la loro profondità.

Chi intendesse utilizzare questa modalità dovrà quindi far precedere la costruzione delle liste dei siti utilizzabili dai bambini da una attenta esplorazione delle varie sezioni e pagine dell'intera struttura del sito.

**Kiddonet™** è interessante soprattutto perché è gratuito: si scarica all'URL http://www.kiddonet.com/knSource/knBrowser.htm. All'inizio esso consente l'accesso solo al progetto omonimo. Starà all'adulto inserire i siti da far navigare al bambino. Iscrivendosi al sito http://www.kiddonet.com/ si possono inoltre usare un sistema di posta elettronica a sua volta protetto e una simpatica agenda e anche costruire una piccola e divertente pagina personale, a sua volta tutelata. Il tutto è in inglese, perché l'ambiente è americano.

**Kid's Internet World Explorer (Kiwe™)**, contempla anche una versione italiana, così come italiane sono le risorse di rete selezionate e proposte. Anche in questo caso il supervisore può intervenire a ampliare o ridurre i siti raggiungibili con un meccanismo basato su password di protezione della "white list". Il programma può essere scaricato in versioni di prova inglese, italiana e spagnola da http://www.kiwe.it/maini.htm e può poi essere sbloccato mediante acquisto di una chiave di registrazione, oppure si acquista nella versione definitivamente funzionante.

Più sofisticata è la metodologia impiegata dal prodotto più recentemente affacciatosi sul mercato dei prodotti per Windows, Il Veliero™ (http://www.ilveliero.info/fam_default.htm): nella versione "famiglia" è free, mentre è a pagamento la versione community. Consente l'accesso una "white list" centralizzata, ma prevede anche la possibilità di aggiungere siti consentiti alle singole utenze "in locale": l'effetto risultante è analogo a quello di un proxy, il controllo consiste in interrogazioni verso una serie di Web Services che esaminano una "white list" di siti "opportuni". La novità consiste nel fatto che, attraverso questo meccanismo, "Il Veliero" può far pervenire una richiesta di attivazione di un nuovo link anche da parte dei vari naviganti, nel momento in cui si trovano di fronte ad un "blocco" di navigazione, motivando l'interesse per il link. Anche di questo ambiente, che consente anche di inibire l'avvio dei browser per adulti presenti sul pc e che si appresta a differenziare i prezzi per l'uso domestico e per quello scolastico, è scaricabile una versione di prova (http://www.ilveliero.info/fam_download.htm).

Amcora si può segnalare **Win-baby**, un sistema di "controllo" dell'insieme delle funzioni del PC, che contiene un semplice browser per bambini, fondato sull'inserimento da parte dell'adulto di parole con cui filtrare, ed eventualmente escludere, le pagine web e della possibilità di compilare liste "bianche" e "nere" di siti. L'ambiente è una specie di shell che si presenta come un sistema operativo, sono presenti anche un client di posta e programmi di scrittura, disegno e di gestione dei files, tutti con interfaccia semplificata. E' possibile implementare il software affinché Win-baby si avvii automaticamente all'accensione ed inibire qualsiasi connessione a Internet, oppure monitorare tempi, siti visitati e mail ricevute e spedite, e quindi configurare il computer in modo globalmente protetto: l'uscita dal software di controllo è infatti possibile solo attraverso l'inserimento di una password e sono inibiti la gran parte dei percorsi da tastiera, fatto salvo l'accesso a "Task manager". **Win-baby** funziona con tutte le più recenti versioni di Windows, ed è scaricabile in versione demo dal link http://www.finson.com/ita/store/comersus_viewItemBundle.asp?idProduct=39 , registrandosi come utenti del sito.

Due pacchetti software interessanti e paragonabili sono **Easybits Magik Desktop** http://www.magicdesktop.com/it/ e **Alice Magik Desktop** http://aiuto.alice.it/offerte/magic_desktop/index.html.
Entrambi creano un ambiente parallelo a quello di Windows (**desktop secondario**) contenente giochi e programmi educativi, senza pericolo di spamming o di virus e senza possibilità di poter modificare file e impostazioni di sistema.
Una volta attivato il desktop secondario da parte del genitore, l'ambiente principale, di cui resta utilizzatore solo l'utente master, non può essere intaccato grazie a una password che ne blinda l'accesso.

Un ulteriore opportunità è rappresentata dall'installazione di software per filtrare i contenuti Internet: il software maggiormente utilizzato è il filtro di Davide.it http://www.davide.it/filtro/presentazione_servizio.php.

**LA NUOVA FRONTIERA: I DISPOSITIVI MOBILI**

L'ambiente d'apprendimento on line comprende non solo Internet, ma anche i telefoni cellulari e le *console* dei video giochi, come ampiamente enfatizzato dai media. Questi dispositivi mobili non sono tecnologicamente controllabili al pari dei personal computer; inoltre, notiamo che i ragazzi sono molto più esperti nell'uso di queste tecnologie dei docenti e dei genitori, ma non hanno le conoscenze per operare in un *ambiente on line sicuro*.
A disposizione degli adulti c'é un'unica risorsa: il dialogo.
Per i telefoni mobili, in particolar modo, cominciano a vedere la luce soluzioni di protezione per la navigazione. Per iPhone c'è Mobicip http://www.mobicip.com/ al costo di 10 $ all'anno, e la versione della 3 del telefonino Apple ha un filtro famiglia incorporato.
I fornitori di connettività telefonica mobile offrono soluzioni di filtro che un genitore può impostare per la SIM del figlio.

**A SCUOLA, MA NON SOLO…**

I possibili mezzi per affrontare i rischi collegati all'uso delle tecnologie on line devono coinvolgere una gran varietà d'attori a livelli differenti, quali la pubblica amministrazione, le organizzazioni per la tutela dei minori, l'industria (fornitori di servizi e di contenuti, produttori di software), le istituzioni educative, le scuole, i genitori e la Commissione Europea.

Alcune norme di base, come non collocare il collegamento ad Internet in un luogo nascosto della casa o non lasciare completamente soli i ragazzini quando navigano, sono norme di buon senso anche molto efficaci. E i vari sistemi di controllo dei contenuti su Internet per la protezione dei bambini e, in generale, dei minori: *parental control* (controllo dei genitori), filtro famiglia, sistemi di etichettatura, *walled garden (*il "giardino recintato" dove si naviga su un Internet limitatamente ad alcuni siti) entreranno sempre di più nell'uso comune delle famiglie.

Per una migliore azione di indirizzo e protezione è utile, sia per la scuola che per la famiglia, conoscere anche istituzioni che svolgono attività correlate a questi temi.

**TELEFONOAZZURRO E HOT114**

E' attiva in Italia una hotline in servizio 24 ore su 24, a cui segnalare, anche in forma anonima, materiale pedopornografico, contenuti razzisti e discriminatori, siti violenti o che istigano alla violenza e tutto ciò che può essere potenzialmente pericoloso per bambini e adolescenti. Si chiama **Hot114** ed è operativa sia attraverso la compilazione di una scheda di segnalazione disponibile sul sito http://www.hot114.it/, sia chiamando il numero gratuito 114 da telefonia fissa, oppure il numero di Telefono Azzurro 19696. Ad accogliere le richieste d'intervento degli utenti ci sono operatori esperti, i quali provvedono immediatamente ad inoltrare la segnalazione alle Istituzioni competenti, tra cui la Polizia Postale, sempre nel rispetto dell'anonimato, per chi lo desidera. Sul sito sono disponibili risorse ed informazioni estremamente interessanti per genitori, docenti e ragazzi.
http://www.azzurro.it/ http://www.hot114.it/
http://www.saferinternet.org/web/guest/home;jsessionid=C82DC635F43F43E453A3BBC015BC2F1D

**MINISTERO DELLE COMUNICAZIONI**

Il Ministero delle Comunicazioni ha inaugurato un rapporto di collaborazione con **Save the Children Italia**, che, attraverso una convenzione, è stata identificata quale partner privilegiato per promuovere attività e elaborare proposte volte alla tutela dei diritti dell'infanzia, sotto il particolare profilo del rapporto del minore e le tecnologie della comunicazione, sia tradizionali che innovative.
http://www.ti6connesso.it/ http://www.savethechildren.it/IT/HomePage

**POLIZIA DI STATO**

http://www.poliziadistato.it/

**AZIENDE**

Grandi aziende del settore ICT sono impegnate nei progetti tesi alla fruizione sicura delle nuove tecnologie da parte dei minori. Tra esse si annovera anche la casa di Richmond. Infatti, Microsoft, con il contributo dell'*Associazione Nazionale Dirigenti e Alte Professionalità della Scuola* http://www.anp.it/usr/index.bfr , è autore del progetto "**Sicurezza on line**". Con tale progetto intende mettere a disposizione dei docenti un percorso di formazione su quattro temi:

- Sicurezza del computer
- Protezione dei dati personali
- Sicurezza dei ragazzi
- Comportamenti on line

I dettagli sul progetto: http://www.apprendereinrete.it/

**RIFERIMENTI NORMATIVI → LA PROTEZIONE DEI MINORI DA CONTENUTI PERICOLOSI**

L. 38/2006 DISPOSIZIONI IN MATERIA DI LOTTA CONTRO LO SFRUTTAMENTO SESSUALE DEI BAMBINI E LA PEDOPORNOGRAFIA
http://www.camera.it/parlam/leggi/06038l.htm
http://www.comunicazioni.it/tutela_minori/

Internet possiede un formidabile potenziale informativo di cui è difficile fare a meno, la possibilità di reperire qualsiasi tipo di informazione, indipendentemente dal contesto socio-culturale a cui si appartiene, costituisce una straordinaria opportunità sociale e didattica.
La normativa italiana è tra le più evolute e consente di attivare strumenti atti ad evitare che i minori accedano, anche involontariamente, a materiali non idonei a soggetti in età evolutiva, che commettano reati o che si isolino a causa di un eccessivo utilizzo di internet.
Tra le istituzioni coinvolte nella diffusione della cultura dell'uso legale e consapevole della rete, spicca l'impegno del *Ministero dello Sviluppo Economico – Comunicazioni*, che dedica uno spazio speciale del suo sito Internet alle politiche per la Tutela dei Minori. Un luogo informativo dove poter trovare le attività, le normative e i consigli utili su un tema di grande importanza e attualità.

**SAFER INTERNET**

Dal canto suo la Commissione Europea ha lanciato una consultazione pubblica per identificare i modi più efficaci per rendere le tecnologie della comunicazione e l'ambiente on line sicuri per gli utenti, in particolare per i bambini. Con il programma **Safer Internet** (Internet più sicuro), alla sua seconda edizione, la Commissione Europea intende porre maggiore attenzione ai fenomeni del **grooming** (adescamento) e del bullismo online.
Il programma 2009-2013 avrà un budget di € 55.000.000. Il nuovo programma assieme alla lotta contro i contenuti illeciti ed i comportamenti dannosi , servirà anche a sviluppare le conoscenze specialistiche in materia di usi esistenti ed emergenti, dei rischi e delle conseguenze delle tecnologie online per la vita dei bambini, compresi gli aspetti psicologici e sociologici dell'esperienza online da parte del bambino.
http://ec.europa.eu/information_society/activities/sip/policy/programme/index_en.htm

**E SE VOLESSIMO METTERE IN ATTO ATTIVITÀ DI "DIFESA" UTILIZZANDO I NORMALI PROGAMMI?**

E' possibile configurare i browser, Internet Explorer, Mozzilla Firefox e gli altri, al fine di controllare il contenuto della navigazione Internet.

Le modalità sono di seguito esplicitate:

Con Internet Explorer in esecuzione clic su STRUMENTI → nel menù che successivamente apparirà, selezionare OPZIONI INTERNET → nella SCHEDA successiva selezionare la voce (in alto a destra) CONTENUTO → CONTENUTO VERIFICATO → scegliere ATTIVA.
Questo parametro ci consente di definire i requisiti che una determinata pagina e/o sito deve avere per potere essere visualizzata nel nostro browser. All'interno della voce: contenuto verificato, fare clic sul bottone **IMPOSTAZIONI** (se è già stata precedentemente attivata, verrà richiesta la password del supervisore ). A questo punto apparirà sul monitor il menù di configurazione del contenuto.
Facendo clic sul bottone: **CLASSIFICAZIONI** , avremo l'elenco dei controlli così suddiviso:

- Contenuto non adatto ai bambini
- Contenuto generato dall'utente
- Contenuto intimidatorio
- Gioco d'azzardo
- Alcool/Droghe/Tabacco
- Linguaggio
- Materiale sessuale
- Nudo
- Violenza

Posizionandoci con il cursore del mouse (tenendo il pulsante sinistro premuto) sul cursore a scorrimento della voce LINGUAGGIO e trascinando lo stesso verso destra, potremo leggere subito sotto (alla voce descrizione) la impostazione dei vari livelli della protezione. Una volta scelto il nostro livello, possiamo passare alla voce successiva e così via sino al completamento delle varie voci. Una volta stabiliti i livelli per il Linguaggio, le Scene di Nudo, il sesso e la violenza, confermare cliccando su **APPLICA** QUINDI **OK**.

All'interno della sezione **SITI APPROVATI** (se lo riterremmo opportuno,quando avremo catalogato i vari siti graditi e non graditi) inseriremo l'elenco dei siti prescelti

La sezione **GENERALE** è molto intuitiva e contiene le impostazioni dell'utente per quel che riguarda principalmente la password ed il suo utilizzo. Consiglio di spuntare la voce: **Il supervisore può inserire una password per consentire la visualizzazione dei siti con restrizioni**. Infatti, così facendo, alla visualizzazione di un sito che è stato censurato, avrete la possibilità (una volta inserita la password che vi verrà richiesta al momento della visualizzazione) di escludere (solo per la sessione odierna) la restrizione e poterlo così visionare.

Non modificate le impostazioni nella scheda **AVANZATE**. Per confermare le scelte è necessario sempre cliccare su **APPLICA** quindi **OK**!

Il parametro CERTIFICATI serve per verificare ed accertare i certificati ed i loro autori; cliccando sul bottone **CERTIFICATI** otterremo l'apertura del menù contenente una serie di dati suddivisi in base allo scopo designato, che può essere: Posta Elettronica protetta, Autenticazione Client, Scopi Avanzati e tutti.
In riferimento allo Scopo designato avremo la possibilità di visionare:

- Personale: (Se non predisposta la sezione è VUOTA)
- Altri Utenti: (Se non predisposta la sezione è VUOTA)
- Autorità di Certificazione Intermedie: contiene l'elenco delle Autorità dei vari Certificati emessi
- Autorità di Certificazione fonti attendibili: contiene l'elenco della autorità dei vari certificati emessi per la categoria

E', altresì, possibile impostare il completamento dei nostri dati durante la digitazione degli stessi all'interno di form, campi e/o interfacce di siti web.
All'interno della sezione, cliccando sul bottone **Completamento automatico**, avremo la possibilità di:

- ☑ Completare automaticamente gli indirizzi web che andremo a digitare: spuntando la relativa casella di spunta
- ☑ Completare automaticamente nome utente e password che andremo a digitare: spuntare la relativa casella di spunta.

Vi suggerisco di non spuntare altre voci: moduli e richiedi salvataggio password. *Un eventuale programma spia potrebbe estirpare questi dati.* Le scelte vanno sempre confermate con la pressione dei pulsanti **APPLICA** ed **OK**.

Un ulteriore strumento, presente da Windows Vista in poi, è **Controllo genitori** consente di gestire l'accesso dei bambini al computer. È possibile, per esempio, configurare impostazioni che pongano ai bambini limiti:

- per quel che concerne l'accesso al Web;
- sulle ore in cui possono utilizzare il computer;
- sui giochi e sui programmi che possono eseguire.

Quando **Controllo genitori** blocca l'accesso a una pagina Web o a un gioco, viene visualizzata una notifica del blocco operato. Il bambino può fare clic su un collegamento presente nella notifica per chiedere l'autorizzazione ad accedere alla pagina Web o al programma bloccato. I genitori possono accogliere la richiesta utilizzando il proprio account. Prima di iniziare, verificare che ogni bambino per il quale si desidera configurare **Controllo genitori** abbia un account utente standard, perché Controllo genitori può essere applicato solo agli account utente standard. Per configurare **Controllo genitori** è necessario disporre di un account utente amministratore. Non è possibile applicare **Controllo genitori** a un account utente amministratore. Per attivare **Controllo genitori** per un account utente standard.

1. Fare clic sul pulsante *Start*, scegliere *Pannello di controllo* e quindi in *Account utente* fare clic su *Impostare il controllo genitori*. Se viene chiesto di specificare una password di amministratore o di confermare, digitare la password o confermare.
2. Fare clic sull'account utente standard per il quale si desidera configurare Controllo genitori.
3. In Controllo genitori fare clic su *Attivo*.
4. Dopo aver attivato Controllo genitori per l'account utente standard desiderato, sarà possibile modificare le singole impostazioni che si desidera controllare. È possibile controllare le aree seguenti:

- **Restrizioni per Internet.** È possibile limitare i siti Web visitabili dai bambini, limitare l'accesso ai soli siti Web adatti alla loro età, impedire il download di file e specificare i tipi di contenuti da bloccare. È anche possibile bloccare o consentire l'accesso a siti Web specifici.

- **Restrizioni di orario.** È possibile impostare restrizioni di orario per definire in che momenti della giornata i bambini possono accedere al computer. Con le restrizioni di orario i bambini non possono accedere al computer nelle ore specificate e, se sono già connessi, verranno automaticamente disconnessi. È possibile impostare ore di accesso diverse per ogni giorno della settimana.
- **Giochi**. È possibile controllare l'accesso ai giochi, scegliere un livello di classificazione per età, specificare i tipi di contenuti da bloccare e negare l'utilizzo di giochi specifici o non classificati.
- **Consentire o bloccare programmi specifici.** È possibile impedire ai bambini l'esecuzione di programmi indesiderati. Dopo aver aperto il **Controllo Genitori**, fare clic sul nome della persona a cui si desidera impedire l'esecuzione di programmi specifici. In Controllo genitori fare clic su *Attivo*. Fare clic su *Blocca programmi specifici*. Fare clic su *nome della persona* **può utilizzare solo i programmi consentiti nell'elenco**. Selezionare i programmi che si desidera consentire. Se il programma desiderato non è presente in elenco, fare clic su **Sfoglia** per individuarlo.

Se si utilizza **Mozilla Firefox**, bisogna partire dalla costatazione che **Firefox** non ha controlli parentali integrati nel pacchetto software di base. Quindi, al fine di impostare i controlli parentali, è necessario scaricare un ***add-on*** che permette di impostare i controlli ed effettuare l'eventuale censura.

Per scaricare un add-on è necessario navigare nella pagina https://addons.mozilla.org/it/firefox/, alla sezione **Privacy e Sicurezza**, quindi scegliere il controllo parentale preferito. I più consigliati sono: Procon Latte, Glubble, Suricate e FoxFilter.

Installare l'add-on scelto. A seconda del filtro selezionato, il metodo per impostare i controlli parentali sarà differente.

Facciamo riferimento all'utilizzo di **Procon Latte**. Dopo aver installato il software, scegliere **Strumenti** nel menu di stato, quindi **Add-Ons**. Selezionare l'add-in, in questo caso **Procon Latte** e fare clic su **Opzioni**. In tale scheda è possibile impostare i "divieti". Per Procon, vai su "*Main Filter*" e spunta "*Enable Explicit Material Filter*". È inoltre possibile modificare il filtro per bloccare tutto ciò che desideriamo sia bloccato. Dopo aver impostato i controlli, l'esperienza Internet dei nostri ragazzi dovrebbe essere un po' più sicura!

Risorse

- https://addons.mozilla.org/it/firefox/ https://addons.mozilla.org/it/firefox/addon/4351

Un altro metodo per migliorare la sicurezza della navigazione dei nostri figli consiste nell'utilizzo di DNS che indirizzano a server "filtrati", che consentono l'accesso solo ai contenuti scelti dal provider.

**Domain Name System** (DNS) è il sistema utilizzato per la risoluzione di nomi di host in indirizzi IP e viceversa. Il servizio è realizzato tramite un database distribuito, costituito dai server DNS. Il nome DNS denota anche il protocollo che regola il funzionamento del servizio, i programmi che lo implementano, i server su cui questi girano, l'insieme di questi server che cooperano per fornire il servizio.

I nomi DNS, o "nomi di dominio", sono una delle caratteristiche più visibili di Internet; l'operazione di convertire un nome in un indirizzo è detta risoluzione DNS.

DNS è, quindi, il servizio normalmente fornito dal provider che converte i nomi di host in indirizzi IP. Il server DNS ha in memoria il database degli indirizzi. Nel momento in cui digitiamo un indirizzo sul browser (es. www.nomesito.it) il server DNS lo converte nel numero a 4 cifre, chiamato Indirizzo IP, corrispondente al sito richiesto. In questo modo il DNS permette la comunicazione tra il nostro PC e il sito.

I DNS sono nati per una questione di comodità: è molto più facile ricordare degli indirizzi alfanumerici (www.etc.) che dei numeri IP (72.14.234.104 invece che www.google.com). Ovviamente l'utente non si accorge di nulla in quanto tutto avviene in modo "trasparente".

E' sufficiente effettuare la modifica con un account da amministratore e fornire account con privilegi da utente alle persone che devono navigare su internet in modo protetto. Se si utilizza un router è sufficiente impostare i DNS ed impedire ai client il traffico sulla porta 53 TCP/UDP..

Con tale sistema è, altresì, possibile consentire navigazioni "protette" anche mediante telefoni mobili.
Indichiamo di seguito alcuni servizi che offrono il servizio di DNS "filtrato":
**ScrubIT** http://www.scrubit.com/ è un servizio Internet che, utilizzando la risoluzione DNS, cerca di filtrare la navigazione internet da siti pericolosi (sono ritenuti tali siti che distribuiscono malware), da contenuti pornografici indesiderati e da errori di digitazione che spesso portano su siti sgradevoli; **ScrubIT** protegge anche dall'accesso a contenuti pornografici o pedo-pornografici.
Come funziona esattamente? Semplice: basta impostare il proprio computer (o il proprio gateway) affinchè utilizzi i DNS di ScrubIT per risolvere gli indirizzi Internet (DNS primario: **67.138.54.100** - DNS secondario: **207.225.209.66**); quando si cercherà di accedere ad un sito classificato "pericoloso", si riceverà un messaggio di blocco.
E' possibile personalizzare la lista dei siti bloccati e consentiti.

**OpenDNS** http://www.opendns.com/ è stato il primo servizio, datato 2006, che aveva lo scopo di rendere la navigazione in rete più sicura.
Per chi volesse impostare gli **openDNS** nella propria connessione i due indirizzi sono DNS primario: **208.67.222.222** - DNS secondario: **208.67.220.220**. Per chi ha bisogno di aiuto sul sito ufficiale può trovare una guida semplice e intuitiva.

Sulla stessa scia dei precedenti **MagicDNS** http://www.magicdns.it/index_it.php un sistema di navigazione controllato. Basato su protocolli standard, **MagicDNS** e' un filtro web che permette una protezione da contenuti web illegali o indesiderati e da minacce informatiche come virus, spyware e malware. Gratuito per le utenze private e le associazioni non-profit, utilizza i seguenti DNS per risolvere gli indirizzi Internet (DNS primario: **95.110.196.200** - DNS secondario: **207.154.16.42**.

Anche Google si è recentemente aggiunto fra i provider che forniscono DNS "filtrati"; gli indirizzi IP dei server sono i seguenti: DNS primario: **8.8.8.8** - DNS secondario: **8.8.4.4**

**MONITORAGGIO DELL'USO DIDATTICO DELLA RISORSA WEB: UNA SOLUZIONE OPEN SOURCE**

## 1. PREMESSA

Con il diffondersi delle Nuove Tecnologie, cresce nelle istituzioni scolastiche il numero di docenti che introducono l'utilizzo del web nei percorsi curricolari. Le attività condotte nel web dal gruppo classe o singolarmente dagli alunni possono grosso modo essere raggruppate in due grandi ambiti: l'*information hunting*, e il *web publishing*.
Nel primo caso, è prevalente il flusso informativo diretto dall'esterno verso la scuola e generalmente consiste nella ricerca di materiali didattici utili per l'apprendimento e la rielaborazione personale o di gruppo (tesine, ricerche, approfondimenti disciplinari, ecc.).
Nel secondo ambito, la prevalenza del flusso informativo si inverte, attenendo a tutte quelle attività con le quali vengono rese disponibili in Internet informazioni dalla scuola verso una possibile utenza di Rete.
Sebbene a questi due ambiti comincino ad affiancarsi progetti *web based* di formazione in rete (e-learning), che tendono a sfruttare Internet soprattutto come scenario d'azione e di interazione didattica, all'interno della scuola l'ambiente del word wide web molto spesso è ancora (e sarà) visto più che altro come vasto contenitore di informazioni.

## 2. QUALE LIBERTÀ?

Qualunque sia l'attività progettata e posta in essere, l'insegnante che voglia utilizzare la tecnologia offerta dalla tecnologia ipertestuale del world wide web, **dovrà interrogarsi sul grado di libertà da conferire agli alunni durante le sessioni di ricerca informativa**, sia in termini di presenza/assistenza che di monitoraggio e contenimento tecnologico.
Elemento primario, a nostro avviso, è la presenza, l'assistenza e la guida del docente durante le sessioni di ricerca, tanto maggiore quanto minore è il grado scolastico nel quale si utilizza la tecnologia web. La possibilità di intervento dell'insegnante è fondamentale sia per la risoluzione (in collaborazione con il personale tecnico, se presente) di eventuali problemi tecnici che per il conseguimento di obiettivi didattico-educativi quali l'ottimizzazione delle modalità di ricerca, l'abitudine a districarsi in un notevole rumore di fondo, il saper valutare la qualità informativa delle fonti reperite sul web, ecc.
Se è vero che l'autonomia di ricerca presenta in sè degli elementi di grande interesse e rappresenta in quanto tale uno degli obiettivi finali, è anche vero che questa non può essere raggiunta senza l'aiuto dell'insegnante. Dal punto di vista del monitoraggio tecnologico, attualmente nelle scuole si possono notare situazioni che sfumano dalla totale libertà tecnologica e d'azione, al monitoraggio passivo, fino in alcuni casi all'esistenza di severe restrizioni nell'uso della risorsa web.
Talora, lo studente può muoversi solo in locale, navigando in un ipertesto preventivamente scaricato dal docente sull'Intranet d'istituto.
**La ricerca "live" sul web presenta elementi di criticità** e non è esente da rischi, quali il naufragio informativo, l'imbattersi in materiale non pertinente, l'abuso del mezzo, l'uso prevalentemente ludico o semplicemente finalizzato alla chat.
Dall'esperienza di molti docenti è emersa la necessità, oltre alla presenza e assistenza "on site", di monitorare tempestivamente le attività condotte in Rete dagli alunni. Tale scelta, pur salvaguardando l'autonomia di ricerca e la privacy, tende a prevenire problemi legati ad un uso improprio dello strumento.

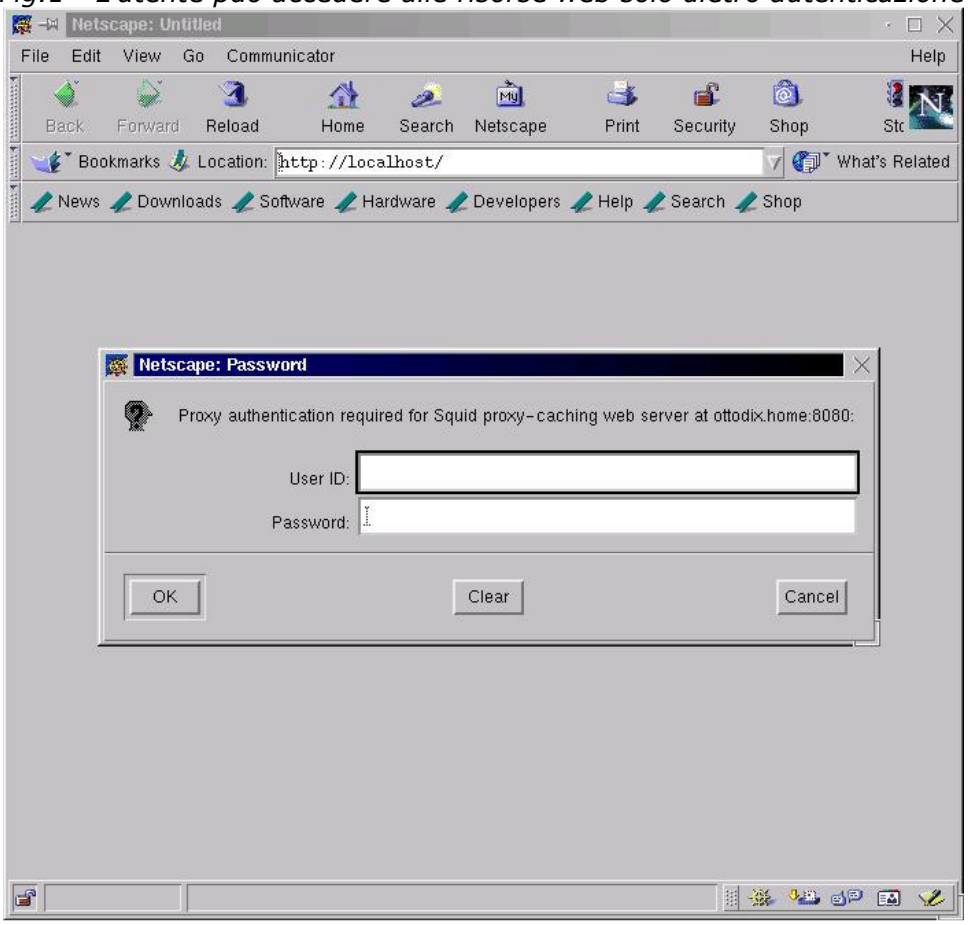
## 3. MONITORAGGIO DELLE ATTIVITA CONDOTTE SUL WEB: UNA SOLUZIONE OPEN SOURCE

La soluzione sperimentata si basa su una soluzione Open Source. Sui notevoli vantaggi rappresentati del Free software e Open Source in ambito scolastico si rimanda alla notevole letteratura esistente on line.
Sulla rete locale della scuola è stato installato un server Linux con funzionalità (tra le varie) di *proxy*. Il proxy tecnicamente è un *firewall* a livello dell'applicazione ovvero, in parole povere, una sorta di intermediario tra gli utenti della rete locale e Internet.

**L'opportuna configurazione del proxy permette di definire delle regole di utilizzo nonché rendere più efficace l'uso del web.**

A tal fine, su una macchina con sistema operativo Linux, nella fattispecie una distribuzione ***RedHat 6.2***, è stato istallato ***Squid***, un proxy estremamente versatile e potente. La sua capiente *cache* permette innanzitutto di salvare sul server le pagine scaricate dagli utenti, rendendole disponibili per ulteriori consultazioni. In una rete scolastica collegata a Internet tramite un router ISDN, quindi con velocità di trasferimento dati verso e da Internet al massimo di 64 kbps, ciò può risultare molto utile. Spesso accade infatti che, attribuito un compito ai ragazzi, molti di loro transitino dalle medesime pagine e se queste sono state precedentemente già consultate da un compagno esse vengono rese disponibili immediatamente (a parte alcuni casi), senza che si occupi banda per scaricarle di nuovo.
Squid ha un file di configurazione che permette di abilitare alla navigazione i singoli client di rete, gli utenti, in quali orari, ecc.
Sul lato client, in questo caso macchine Windows 9x, il browser deve essere configurato per puntare alla porta del proxy. Un'alternativa è quella di utilizzare la modalità di "proxy trasparente", ovvero reindirizzando sul server il traffico generato dai client sulla porta del proxy senza che l'utente si accorga di nulla; in tal caso bisogna settare come gateway il server e non il router ISDN. In ogni caso comunque per mettere in sicurezza i settaggi di rete si può utilizzare il software Poledit fornito da Microsoft con il sistema operativo Windows.
Si è scelto di permettere agli utenti di accedere alle pagine web **solo dopo essersi autenticati** (Fig.1). Questa semplice misura generalmente porta alla responsabilizzazione dell'utente, oltre che permettere, ove necessario, l'individuazione degli abusi. Squid permette l'utilizzo di diversi sistemi di autenticazione esterni. Nel caso in oggetto è stato scelto il sistema di autenticazione NCSA (incluso nei file sorgente di Squid), con un controllo direttamente sul file delle password /etc/passwd. Per l'amministratore di rete, nel nostro caso il docente referente del laboratorio, ciò semplifica la vita perché una volta creato un utente per l'accesso alle risorse condivise sul server (directory di transito, homes personali, servizi di stampa, ecc.) lo stesso userid e password saranno automaticamente quelle che l'utente dovrà utilizzare anche per accedere a Internet.

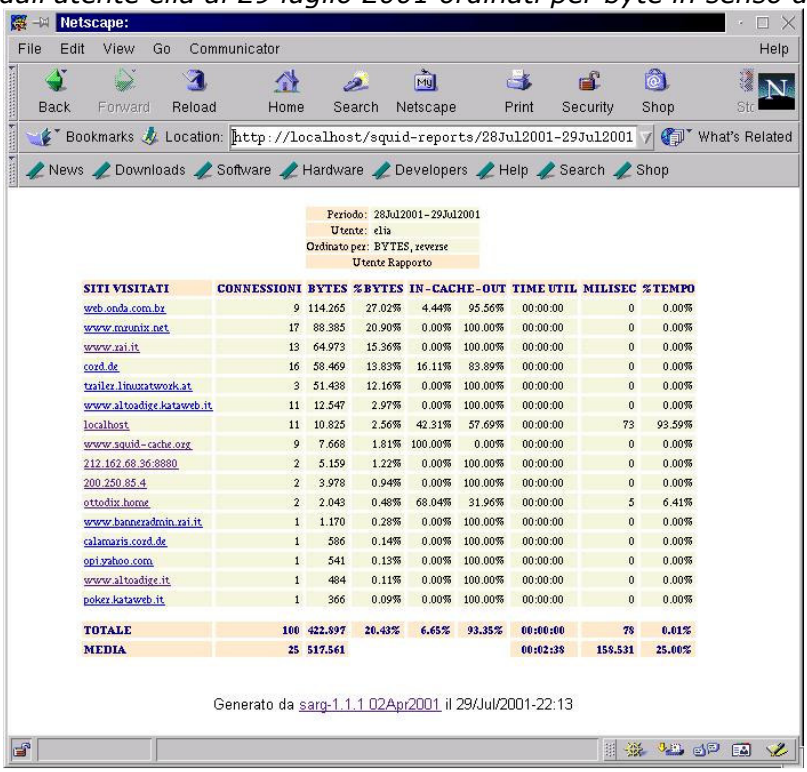
*Fig.1 - L'utente può accedere alle risorse web solo dietro autenticazione*




Periodicamente, il responsabile di laboratorio, può controllare sul server i siti visitati agli alunni consultando i file di log di Squid. Data la complessità dei file di log in questione, viene utilizzato

un apposito analizzatore (ma se ne possono reperire parecchi altri in Internet), ***Sarg*** (Squid Analysis Report Generator). Una volta lanciato, Sarg genera un rapporto in html consultabile dal responsabile (o da tutti) sul sito Intranet del laboratorio con nomi utenti, date e orari, indirizzi numerici dei client e siti web visitati (Fig.2).

*Fig. 2 - Sarg, uno dei tanti analizzatori di log di Squid. Nell'esempio i siti web visitati dall'utente elia al 29 luglio 2001 ordinati per byte in senso decrescente*

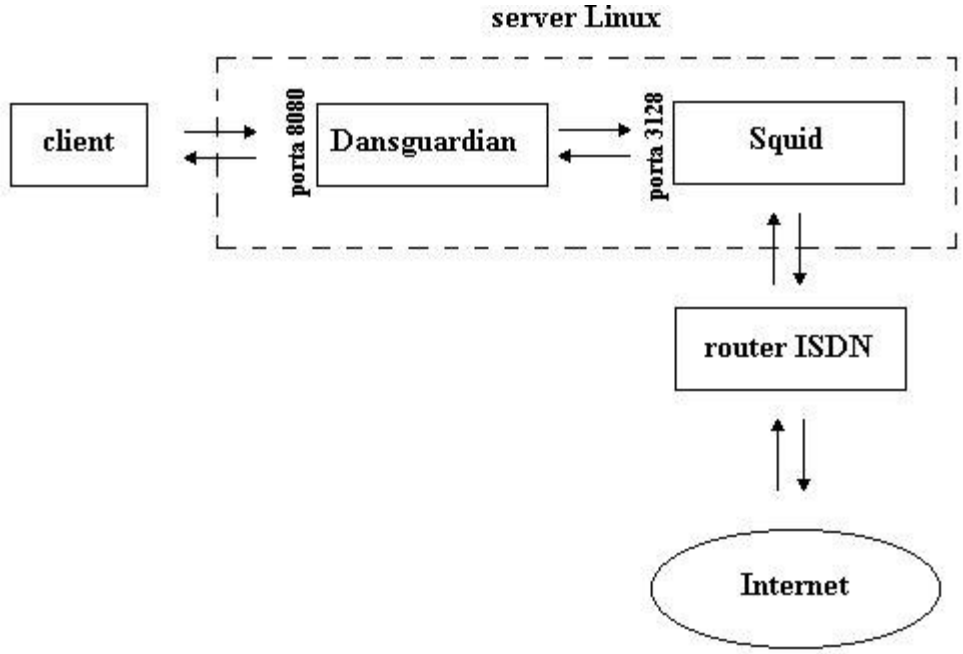



***^top***

## 4. UNA SOLUZIONE "ESTREMA": IL FILTRAGGIO DELLE PAGINE

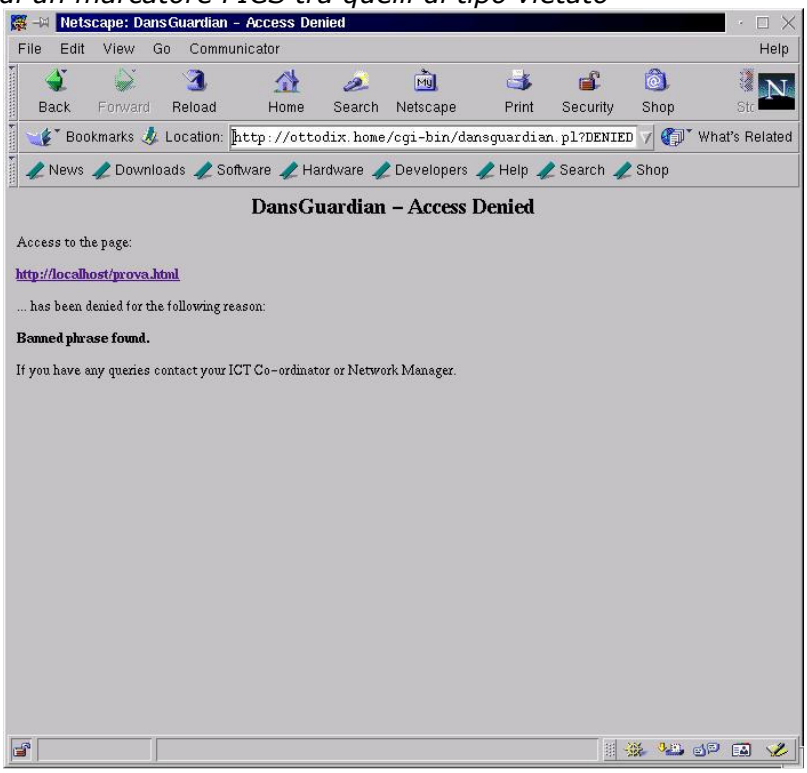
A livello sperimentale, non tanto per il riscontro di reali esigenze di filtraggio, è stato deciso di installare sul server del laboratorio ***Dansguardian***, un software molto interessante concepito appositamente per la scansione dei testi delle pagine web visitate. Esso frapponendosi ulteriormente tra l'utente e Squid (Fig. 3), permette l'analisi in tempo reale dei contenuti visitati.

*Fig. 3 - Schema semplificato del percorso compiuto dalla pagina web*




In pratica, l'utente chiama dal browser una pagina web in Internet, la richiesta viene intercettata da Dansguardian quindi passata al proxy che, una volta ottenuta (da Internet o dalla cache, se è già stata visitata) la passa di nuovo a Dansguardian, che la esamina. Se viene riscontrata la presenza di una o più parole chiave (o di una loro una combinazione) la pagina viene bloccata (Fig. 4), altrimenti viene regolarmente visualizzata sul client che l'ha richiesta. E' compito dell'amministratore della LAN scolastica definire una lista di "parole sensibili" e la risposta che il server deve generare una volta incontrata una di queste parole (pagina di avviso, reindirizzamento, ecc.). Dansguardian presenta comunque la possibilità di scansione delle pagine attraverso i marcatori PICS similmente ad altro software presente in commercio.

*Fig. 4 - Dansguardian ha rilevato la presenza nella pagina di una determinata parola chiave o di un marcatore PICS tra quelli di tipo vietato*



Seguendo alcuni esempi europei, se nelle scuole sorgessero esigenze di filtraggio, si potrebbe creare un gruppo di lavoro che si occupi collegialmente della definizione delle regole di filtraggio, in modo tale da dare assistenza ai docenti che volessero sperimentare il sistema.

**5. NOTE TECNICHE**

Infine, alcune informazioni tecniche sul server. Per rispondere in tempi brevi alle richieste dei client di rete e minimizzare i tempi di gestione della cache, la macchina che funge da server deve essere sufficientemente dotata di RAM e avere un disco rigido veloce. La macchina utilizzata come server è un Pentium II con 128 MB di RAM e HD da 20 GB. Sistema operativo installato: ***Linux RedHat 6.2***. Software Open Source utilizzato: ***Apache 1.3.20*** come server web dell'Intranet, ***Samba 2.0.7*** per la condivisione di risorse di rete (autenticazione utenti, accesso a spazi disco personali e collettivi, stampanti), ***Squid 2.4.STABLE1*** come proxy (autenticazione pr accesso al web e caching delle pagine web), ***Sarg 1.1.1*** per l'analisi dei file di log di Squid e report in HTML, ***Dansguardian 1.0.0*** per il filtraggio delle pagine web, Webmin per la manutenzione e gestione in remoto del server dalla macchina del docente (aggiunta utenti, creazione share, gestione delle code di stampa, lancio programmi ecc.).