Guida essenziale per genitori e maestri sulla sicurezza nella navigazione Internet

Campagna di diffusione dell'informazione sui sistemi di tutela della navigazione dei minori per la prevenzione della pedofilia e della pedo-pornografia nelle scuole primarie di Roma

condotta da

Associazione Centro ELIS

finanziata dalla

FEO - FIVOL

della FONDAZIONE ROMA

nell'anno scolastico 2008-9

Un messaggio a genitori e docenti

Il computer è entrato a far parte delle nostre famiglie e delle scuole con una facilità che solo pochi anni fa non ci saremmo aspettati. Ma la caratteristica che accomuna tutti i PC (e ormai anche molti telefoni cellulari) è la sua connessione a Internet, la rete mondiale che permette comunicazioni istantanee di dati, ricerca veloce di contenuti, acquisti e tanti servizi di informazione. Sicuramente Internet è uno strumento informativo, mentre resta da dimostrare che sia anche formativo, soprattutto per i più giovani. Va accompagnato da cautele che sono tipiche di tante risorse utilissime nella vita di ogni giorno: l'energia elettrica è un esempio tanto importante quanto pericoloso se mal gestito.

In questa guida essenziale ci soffermeremo sugli aspetti negativi e sui rischi, senza togliere nulla alla positività di Internet che è diventato indispensabile e quasi irrinunciabile. Un glossario finale aiuta alla comprensione dei termini tecnici e gergali.

Controllare non vuol dire proibire a priori. Anche se ci sono pericoli, è necessario insegnare ai bambini ad affrontarli, così come si insegna loro ad attraversare la strada e a difendersi dalle infezioni, con semplici misure di prudenza e prevenzione.

Tenere i bambini completamente isolati dai microbi non favorisce lo sviluppo di anticorpi e rischia di fare molto danno al primo impatto involontario con un agente patogeno. Non serve perciò tenerli del tutto lontani da Internet: bisogna invece educarli ad affrontare la rete con spirito critico, gradualmente, dando loro la giusta dose a ogni età. Dobbiamo scegliere le fonti di informazione adatte a loro, così come si scelgono i libri per insegnare le diverse materie in base alle loro capacità di comprensione.

Questo è il compito di noi educatori ma, purtroppo, ci troviamo per la prima volta nella storia a saperne di meno degli studenti. Ci si chiede perciò uno sforzo aggiuntivo che sarà premiato dalla formazione di una generazione di futuri adulti capaci di acquisire conoscenze in modo consapevole senza rischiare una nuova schiavitù culturale.

Michele Crudele, 31 ottobre 2008

Comportamento on-line

Esiste la necessità di regole anche nei rapporti *on line*, cioè sulla rete che collega i *computer* nel mondo. Nel passaggio dal televisore al PC spesso ci si pone con lo stesso spirito di intrattenimento passivo. Ma basta poco per accorgersi che con il *web* la nostra esperienza può invece acquisire connotati molto più attivi. Su Internet, nel *World Wide Web* possiamo dare le nostre generalità, esprimere un parere, scegliere una *password*, lasciare un commento, giustificarci o accusare, pubblicare foto e filmati.

Vediamo la nostra casella di posta elettronica come il nostro piccolo regno privato anche se sappiamo che le *e-mail* sono esposte a varie forme di indiscrezione. Inoltre il nostro indirizzo *e-mail* ci viene di solito chiesto per accedere ad un qualsiasi servizio presente nella rete. Abbiamo insomma una serie di ambienti in cui il nostro comportamento ci espone al giudizio degli altri, nelle *chat*, nei *forum*, nei *blog* e negli altri ambienti di condivisione. Per questo la codifica di alcune norme di comportamento nella *netiquette* è di grande importanza: seppure sconosciuti i nostri *partner* in rete si fanno un'idea di chi siamo e di quali sono i nostri valori di riferimento e atteggiamenti.

Anche in Internet occorre rispettare gli altri e pretendere di essere rispettati. Occorre rinunciare a forme di anarchia, per imparare tutti a rispettare il comportamento corretto degli altri. Nessuno deve prevaricare sugli altri, neanche se ha maggiori conoscenze tecnologiche. Purtroppo c'è anche chi utilizza la rete per far valere la propria presunta forza a danno di chi è più giovane e indifeso: è il cyberbullismo.

Cyberbullismo

Il naturale e antico esibizionismo dei bulli trova uno sfogo eccezionale nei mezzi di comunicazione offerti dalla rete. Sembra di trovarsi di fronte all'amplificazione, tramite il *web*, di una reale trasgressione che in altri momenti e in altri contesti sarebbe rimasta circoscritta fra le pareti scolastiche. Il cyberbullismo è un fenomeno in via di espansione. Nella vita reale il bullismo di solito si manifesta come un'azione di gruppo, elaborata a soli fini di divertimento ma che può avere anche conseguenze molto gravi.

In Internet invece più frequentemente è un'azione solitaria, che si verifica in prevalenza nelle chat o via *e-mail*. Un modo per sconfiggere questa forma di stupidità molto spesso è il silenzio. Ignorare la prepotenza è un modo per renderla vana: la migliore difesa è non fare nulla. Se il fenomeno persiste, conviene parlarne: i ragazzi devono dirlo agli amici, ai genitori, agli insegnanti. Non conviene invece amplificare troppo gli episodi di bullismo per evitare di soddisfare il desiderio di notorietà dei bulli.

Dal plagio alla condivisione

Cercare su Internet è un compito sempre più complesso, a causa del moltiplicarsi delle fonti e a causa dell'affermarsi del *web* 2.0, cioè della crescita di

pagine interattive, contenenti documenti testuali, audio e video, che possono essere caricati e scaricati liberamente.

L'avvento di Internet ha reso più facile e quindi più diffuso il fenomeno del plagio attraverso il copia e incolla. Internet e i motori di ricerca mettono a disposizione istantaneamente le conoscenze che servono, e questo aiuta anche gli studenti che non amano consultare libri di testo o enciclopedie. Paradossalmente, Internet anziché favorire la diffusione della conoscenza, sembra in molti casi favorire solo l'imbroglio. È opportuno avvertire gli alunni e i figli che oltre ad essere una pratica disonesta senza vantaggi reali per la propria cultura, è anche abbastanza facile da smascherare.

Una maggiore diffusione di Internet nella scuola può rafforzare le capacità vere di ricerca, ampliare un corretto spirito di valutazione critica, e rendere quindi inutile compilare pagine interamente copiate. L'obiettivo finale è trasformare gli studenti da lettori e "copiatori" in generatori di contenuti, in produttori di cultura su Internet per metterla a disposizione di tutti.

Sicurezza dei ragazzi

Gli elementi della sicurezza dei ragazzi durante le attività *on line* non sono sempre valutati in maniera adeguata. Gli stessi genitori non vi prestano la dovuta attenzione. La navigazione in Internet è del resto un'esperienza nuova e i giovani navigatori della rete mal tollerano regole e codici. Del resto, soprattutto per gli adolescenti, appare assurda l'idea che si possano imporre delle limitazioni in un terreno in cui la libertà sembra essere incondizionata. Spesso la rete e l'esperienza di Internet è cresciuta insieme ai nostri ragazzi, giorno dopo giorno, senza un'educazione. La maggior parte dei genitori, sul piano delle abilità tecnologiche, è inferiore ai propri figli. È necessario uno sforzo degli adulti di conoscere i linguaggi digitali per poter dialogare con i giovani ed essere in grado di stabilire regole efficaci sin dall'infanzia, senza l'atteggiamento censore, ma con una giusta protezione dai rischi.

Il problema non sono le tecnologie ma i contenuti, spesso contrari alle esigenze di crescita dei nostri ragazzi. I ragazzi sono nati con il *web* e ne vivono le contraddizioni e gli sviluppi: accade spesso che la loro percezione dei pericoli legati a Internet sia superficiale.

I genitori, distratti dai tanti problemi del vivere quotidiano, sono a volte portati a trascurare la portata di alcuni pericoli che attraverso la rete possono seguire i figli fin nelle mura domestiche. L'impiego di *chat* e *forum* possono servire ad accrescere le conoscenze e ad ampliare le situazioni di divertimento, ma possono costituire un pericolo, soprattutto nella preadolescenza.

I luoghi della navigazione

Il primo ambiente su cui riflettere è la collocazione in casa e a scuola del computer normalmente utilizzato per la connessione a Internet. È opportuno

individuare un luogo accessibile a tutti i membri della famiglia, in modo che un potenziale adescatore, al corrente di tale soluzione, sia dissuaso da approcci insidiosi.

In generale i ragazzi, soprattutto i più piccoli, non dovrebbero navigare in Internet da soli nella propria stanza. Esattamente come la televisione, la compagnia di un adulto durante le esplorazioni sul *web* può consolidare la presa di coscienza critica. Può essere opportuno anche limitare il tempo di connessione e sperimentare gradualmente i vari aspetti della Rete e dei suoi strumenti. È opportuno che il bambino si abitui a condividere le proprie conoscenze, a usare una casella postale non esclusiva, a entrare in chat con l'assistenza dell'adulto.

Questo approccio del *web* fatto attraverso una scoperta comune ragazzo-adulto, soprattutto se adottato fin dai primi anni, può porre le premesse per una crescita che potrà svilupparsi negli anni successivi e può prevenire ambiguità e delusioni che si potrebbero creare in seguito.

A scuola è particolarmente consigliata una collocazione (per esempio a ferro di cavallo) che consenta al docente di vedere in un colpo d'occhio tutti gli schermi.

I siti *web*

I siti *web* non sono tutti uguali: ci sono siti dedicati alla diffusione della conoscenza e alla solidarietà, siti dai contenuti offensivi, violenti o a forte carica sessuale.Molti dei siti non adatti alla giovane età ricorrono a trucchi per farsi notare, come le finestre a comparsa (*pop-up*) o anche l'occasionale errore di digitazione che porta il navigatore verso trappole.

Per proteggere la navigazione nelle scuole dovrebbero essere usati dei filtri che bloccano l'accesso a pagine contenenti determinate parole o argomenti. In casa sarà compito dei genitori contrattare l'utilizzo di tali strumenti e il rispetto di regole di navigazione fin dai primi anni, altrimenti ci si può trovare di fronte a rifiuti perentori.

Le *community*

Su Internet i nostri ragazzi non consultano solo dizionari o enciclopedie o pagine dei cantanti preferiti, ma hanno anche l'opportunità di costruirsi un'identità, di presentarsi al mondo, e di instaurare rapporti di vario tipo. È importante che la *community* di cui entrano a far parte sia sana e interessante, oltre che divertente. È bene che anche in questa fase un adulto segua questa iniziazione alla vita sociale in Rete e sia compagno di viaggio soprattutto nelle prime fasi di queste esperienze.

Al momento dell'iscrizione a una *community* non deve comunque mancare l'assistenza di un adulto, che sappia valutare le condizioni di *privacy* e di impiego dei dati personali offerti. Vi sono poi *community* con obiettivi delimitati, per esempio orientate solo al gioco. Occorre prestare particolare attenzione: è possibile che si infiltri anche qualche adulto con secondi fini, non sempre onesti.

Le *chat*

Le *chat-room* e la messaggeria istantanea sono molto frequentate dai ragazzi. Purtroppo nessuno ha gli strumenti per scoprire se chi è in *chat* è veramente chi dichiara di essere. Attenzione dunque ai potenziali brutti incontri, perché è proprio in *chat* che possono nascondersi pericolosi adescatori soprattutto sessuali che, con tecniche subdole, potrebbero indurre il bambino anche ad accettare un incontro in presenza.

Tra i suggerimenti più importanti che possono essere dati ai genitori per la prevenzione del crimine, c'è quello di mantenere un dialogo aperto, una confidenza continua che porti alla condivisione di una serie di regole per fare in modo che eventuali malintenzionati non abbiano accesso alle vite e alle intelligenze dei giovani. I complimenti eccessivi, le offerte di regali e di gadget, l'interesse per avere indirizzo e numeri di telefono, sono sintomi che a volte i ragazzi non accolgono con sospetto, come invece dovrebbero.

Il vantaggio delle relazioni virtuali consiste proprio nel fatto che spesso si possono troncare sul nascere senza pericolose conseguenze. Ma la prudenza non è mai troppa.

Alla *chat* possono essere dedicati approfondimenti anche a scuola, perché tale strumento, come si intuisce, può essere usato anche con finalità didattiche: ad esempio per rafforzare e motivare l'apprendimento delle lingue straniere. È possibile scambiare opinioni ed esperienze con partner internazionali, pianificare l'uscita di un giornalino, fare considerazioni su feste e scadenze tipiche di ciascun paese, scambiarsi informazioni geografiche con scuole gemellate sparse per il pianeta.

L'uso della *chat* e della videoconferenza sembra sottrarre tempo alle normali lezioni, ma le ricadute sull'apprendimento – non solo della lingua straniera – possono essere notevoli. Inoltre l'uso scolastico può valorizzare gli impieghi produttivi e positivi di questo strumento allontanando da eventuali utilizzi a rischio di incontri deleteri.

Il *social networking*

I diari *on line* (*blog*), i *wiki* e le piattaforme di condivisione di contenuti sono tra i fenomeni più interessanti attuali, raggruppati sotto il nome di Web 2.0. Hanno attirato molto i giovani, soprattutto gli adolescenti, YouTube, Facebook, MySpace, Live Spaces e altri simili.

Con un *blog*, ognuno può avere un proprio sito in cui scrivere anche giornalmente e persino tramite SMS, senza alcuna conoscenza tecnica, i propri pensieri, le proprie aspirazioni, le proprie esperienze, anche lasciando ai visitatori l'opportunità di aggiungere commenti. Occorre fare attenzione perché si rischia di rivelare dati personali che dovrebbero rimanere riservati, sia come singoli, sia come famiglia.

Pubblicare foto, filmati e propri commenti significa abbandonare a chiunque quei contenuti che poi non potranno più essere cancellati definitivamente: non

sappiamo chi se ne è appropriato. Cosa succederà a un ragazzo di oggi che tra quindici anni cercherà un'occupazione? Probabilmente il suo potenziale datore di lavoro andrà a cercare su Internet notizie del suo aspirante dipendente, magari partendo dalla sua fotografia: ora non si può trovare una persona partendo dal suo volto, ma in futuro è molto probabile che ci si riesca, così come quindici anni fa sembrava impossibile quello che facciamo ora con Google. Quindi suggeriamo prudenza ai ragazzi prima di pubblicare.

Peggio ancora è l'abitudine di alcune ragazzine di inviare proprie foto oscene in cambio di ricariche di cellulare. A parte gli aspetti morali, indubbiamente importanti, questa prostituzione virtuale può portare a situazioni molto dolorose: per esempio, alla vigilia del matrimonio, la futura sposa può essere ricattata con la minaccia di far vedere le foto al futuro marito oppure se le trova pubblicate su Interent.

Il *wiki* è un sito che consente la costruzione di documenti unitari, ad esempio per stilare uno statuto, un dizionario, un qualcosa che può essere condiviso all'interno di un gruppo. La Wikipedia è il caso più conosciuto perché ormai la ricerca di qualsiasi parola su Google mostra quasi sempre al primo posto una voce di questa enciclopedia gratuita scritta da chiunque. Di per sé è inaffidabile, perché i contenuti non sono controllati da esperti: in qualsiasi momento posso pubblicare una menzogna senza che nessuno mi blocchi. Di fatto è molto valida perché la gente che ci scrive cerca di correggere gli errori, partendo dal principio che si scrivono solo fatti e non opinioni. A parte qualche fanatico, si dimostra una risorsa utile, ma bisogna insegnare ai bambini e ai ragazzi a capire come è fatta e quanto ci si può fidare. Il modo migliore è stimolarli a scrivere sulla Wikipedia, ad aggiungere dati e correggere errori: così comprenderanno meglio il valore vero dei contenuti.

La protezione dei *computer*

L'aumento di potenza dei *computer* non è stato accompagnato da una maggiore sicurezza. La complessità del *software* fa sì che siano frequenti errori che permettono intromissioni indebite nei *computer* di ignari utenti. Oltre ai virus informatici creati per danneggiare i dati, per cattiveria o vendetta, ci sono tutti i *malware* che svolgono operazioni illecite all'insaputa dell'utente normalmente con finalità economiche.

Le strategie principali per evitare manomissioni al *software* del *computer* sono le seguenti:

- Aggiornare con regolarità il sistema operativo, attivando il sistema di avviso automatico degli aggiornamenti.
- Installare un programma antivirus e mantenerlo sempre aggiornato attivando il meccanismo automatico; ne esistono di gratuiti e a pagamento con poca spesa.
- Utilizzare un *firewall*: per Windows XP e Vista è incorporato nel Centro Sicurezza PC; esistono alternative anche gratuite.
- Usare *anti spyware* come Windows Defender o altri anche gratuiti.

- Su Windows Vista o Mac attivare il Controllo genitori incorporato se il *computer* è usato anche dai bambini. Esistono anche alternative, gratuite o a pagamento.

Lo *spam* e il *phishing*

L'invio di posta pubblicitaria non richiesta, chiamata *spam*, è finalizzato a raggiungere il massimo numero di utenti, contando sui grandi numeri per ottenere che alcuni "abbocchino" alla proposta e acquistino il bene in vendita, che spesso è una truffa o non è di qualità. Non conviene mai rispondere ai messaggi di *spam* per evitare di far capire al mittente che il messaggio è stato letto: ne invierà molti altri. Il comportamento corretto è cancellarlo subito e non comprare mai da chi propone qualcosa con un messaggio non richiesto.

Ormai tutti i sistemi di posta elettronica su *web* hanno un *antispam* incorporato che va attivato in ogni caso, anche se c'è il rischio (basso) di far finire nel cestino posta valida che il programma interpreta erroneamente come *spam*: sono i falsi positivi.

Una misura di prudenza è pubblicare su Internet (nei *forum* o *blog*) un proprio indirizzo di posta elettronica dedicato alle comunicazioni pubbliche, mentre quello destinato alla corrispondenza personale resta conosciuto solo da amici, colleghi e parenti.

A volte lo *spam* sembra provenire da indirizzi di amici o nostri corrispondenti o addirittura da noi stessi: è un imbroglio, perché è facile falsificare il mittente. Non dobbiamo fidarci se il contenuto è sospetto: spesso contiene anche trappole come virus o "cavalli di Troia". In ogni caso, non fare mai *clic* sui collegamenti contenuti in questi messaggi. Si tratta spesso di *phishing*, storpiatura della parola inglese che vuol dire "pescando": in questo caso si tratta di pescare i dati personali e i soldi altrui. Si riceve un messaggio di posta elettronica che invita a controllare il proprio conto corrente bancario *on line* perché –dicono– c'è stato qualche problema. Nel messaggio ci sono dei collegamenti a pagine che assomigliano molto a quelle della nostra banca, ma in realtà sono trappole che catturano le nostre credenziali.

Frequenti sono anche le "catene di Sant'Antonio" o le varie "bufale" con storie patetiche o avvisi terrificanti di danni al *computer*. Bisogna diffidare sempre di questo canale di comunicazione: non arrivano via *e-mail* queste notizie. Quelle autentiche si leggono sui portali importanti. In ogni caso va evitato di inoltrare a molta gente un messaggio ricevuto e, soprattutto, mai bisogna mettere gli indirizzi dei destinatari nella casella "A" o "Cc" per motivi di *privacy*. I destinatari non devono conoscere gli indirizzi degli altri, per cui nel caso di una lettera circolare conviene mettere i destinatari in "Ccn" (copia carbone nascosta).

Il furto d'identità

I siti studiati per attrarre l'attenzione dei bambini, con tanti colori, giochi, animazioni, personaggi-guida simpatici e divertenti, oggi si fanno sempre più interattivi e offrono servizi che richiedono una procedura di registrazione.

Di solito occorre fornire almeno un indirizzo *e-mail* per ricevere una password. Per alcuni siti, occorre invece una qualificazione più precisa, e sono richiesti altri dati: nome e cognome, indirizzo privato, numero di telefono, data di nascita, ecc. Alcuni di questi dati servono proprio per garantire la sicurezza dell'accesso e sono spesso conservati anche nel *computer* dell'utente che si è registrato.

Proprio sfruttando questa situazione i ladri di identità agiscono, in due modi diversi:

- Nel momento della trasmissione dei dati al sito da parte dell'utente. In questo caso i malintenzionati sfruttano le debolezze del *browser* non aggiornato.
- Attraverso intrusioni nel *computer* dell'utente: in questo caso il malintenzionato utilizza appositi *software* che si infiltrano in "porte" lasciate aperte nel *computer* del malcapitato.

In entrambi i casi il risultato è lo stesso: i dati personali dell'utente, che gli permettono ad esempio l'accesso al conto bancario *on line*, sono carpiti e utilizzati per compiere furti.

Purtroppo i dati personali "fanno gola" a troppi! Non solo ai ladri e ai truffatori, ma anche ai pedofili. Vi sono occasioni di furto d'identità anche nelle *chat* e nei *forum*, e forse sono le più pericolose, in quanto, più che impadronirsi di chiavi di accesso, lo scopo è spesso quello di stabilire contatti diretti, a sfondo sessuale.

Il furto di identità in Internet è un fenomeno in espansione e probabilmente si porrà con forza sempre maggiore, data la crescita del *Web* 2.0. Per i ladri di informazioni anche un *hard disk* formattato in maniera veloce e poi rottamato può essere una vera manna. Sono molti i dati che gli esperti di informatica possono ricavare da vecchi dischi fissi di *computer*: dati personali, *password*, identificativi per l'accesso a siti o pagine personali, ecc.

Usando le dovute cautele, si può benissimo continuare a fare acquisti su Internet: basta adottare le opportune precauzioni.

Alcune cautele da usare

- Non rivelare mai i dati personali: mai dare il numero di telefono o il proprio indirizzo a chi non conosciamo bene.
- Evitare di rispondere a *e-mail* non richieste. Non fare mai clic sui collegamenti che affermano di aprire il sito della nostra banca: è meglio aprire da soli il *browser* e scrivere a mano la URL esatta della banca.
- Nelle *chat*, nei *forum*, nei profili, scegliere *nickname* generici, dai quali non sia possibile risalire direttamente alla propria identità reale.
- Per proteggere intrusioni nel proprio *computer*, utilizzare *firewall*, *antivirus* e *anti spyware*.
- Distruggere accuratamente i documenti generati dalle nostre stampanti, prima di buttarli nella spazzatura; aumentano anche in Italia coloro che dalla spazzatura ricavano dati sensibili, firme, numeri preziosi per le loro truffe.

- Controllare periodicamente il proprio conto bancario, in modo da individuare movimenti sospetti.
- Conservare in un luogo sicuro una copia del numero di carta d'identità, patente, passaporto, carta di credito, bancomat, ecc. per poter più facilmente sporgere denuncia e bloccarne l'uso.
- Non usare mai *password* troppo facili. Devono essere lunghe almeno sei caratteri, mescolando lettere e numeri ed evitando quelle ovvie, come il cognome della madre, o la propria data di nascita, o il numero di telefono. Non usare la stessa *password* per tutti i servizi in rete per evitare che chi la scopre su uno dei siti possa avere accesso a tutti gli altri. Distinguere soprattutto quella usata per l'accesso al conto in banca.
- Convincere i nostri ragazzi di non accettare proposte di appuntamento da persone conosciute in rete.
- Non rispondere a messaggi improvvisi durante la navigazione che avvisano che il nostro *computer* non è protetto: sono trappole che invitano a installare presunti antivirus che in realtà sono *spyware* o "cavalli di Troia".

I bambini e i ragazzi, senza leggere alcun manuale d'uso, sanno cavarsela con telefonini, lettori DVD e *computer*. Genitori e insegnanti restano ammirati da tale disinvoltura; a volte, di fronte a qualche procedura un po' troppo complessa, si rivolgono a loro per avere delle consulenze. Questa facilità non è sempre seguita da un'attenzione nei confronti dei rischi: la tipica audacia giovanile – che a volte è temerarietà – si manifesta anche su Internet.

È necessario aumentare il livello di competenza degli educatori per evitare danni, oltre che alla salute psichica dei ragazzi anche alle finanze domestiche. Per i ragazzi, "scaricare" un brano musicale senza pagarlo può valere più della mezz'ora di lavoro che occorre per reinstallare il sistema operativo eventualmente andato in *crash* a causa di un virus contenuto nel "pacchetto" della canzone.

Il P2P

La pratica del *peer-to-peer* (P2P), ossia lo scambio di file da *computer* a *computer* supportati da adeguati programmi, può avere diverse finalità. Il P2P praticato dai nostri ragazzi non è sempre finalizzato allo scambio di materiali prodotti autonomamente bensì di *file* (brani musicali, film, interi libri) soggetti a *copyright*. In questo caso si ha una violazione delle leggi sul diritto d'autore. È bene quindi informare i ragazzi sui rischi legali cui vanno incontro o cui fanno andare incontro i propri genitori. Le sanzioni vigenti prevedono anche conseguenze penali perché chi scarica mette, seppure involontariamente, in condivisione quanto scaricato – per la struttura intrinseca del *software* P2P – e quindi si rende colpevole di diffusione del materiale digitale sottratto.

GLOSSARIO

Attivazione
Procedura indispensabile, connessa all'installazione di alcuni software (per esempio Windows XP) per attestarne la genuinità.

Browser
Il programma che permette la navigazione su Internet.

Cavallo di Troia
Programma invisibile che esegue operazioni all'insaputa dell'utente mentre scrive sul suo *computer:* ad esempio cattura dati personali e *password*, inviandoli a malintenzionati. Si installa involontariamente rispondendo ingenuamente di sì a richieste arrivate via *e-mail* o navigando su siti trappola (in genere pornografici).

Copyright
È il diritto d'autore per l'ordinamento legale americano e anglosassone.

Craccare
Neologismo gergale da *crack*, "spezzare". Si intende il superamento delle protezioni di un programma o di un sistema informatico.

Cracker
Pirata informatico, in grado di disabilitare protezioni o infiltrarsi nei sistemi informatici per finalità illecite.

Disclaimer
"Esonero di responsabilità". L'insieme delle condizioni di utilizzo: diritti e doveri dell'utente, limitazioni di responsabilità del produttore, relative a un *software*, da accettare al momento dell'installazione.

DRM (Digital Right Management)
Sistema di gestione dei diritti sulle opere protette da *copyright*.

Fake
"Falso". Utilizzo di un'identità falsa o altrui, oppure *file* designato in modo diverso dal reale contenuto oppure allarme relativo a virus inesistente.

File sharing
"Condivisione dei *file*". Lo scambio dei *file* di solito attraverso reti paritarie (P2P), ma anche attraverso apposite piattaforme. Può essere illegale.

Firewall
Programma o *computer* che permette di evitare l'accesso non autorizzato dall'esterno alla rete domestica, dell'azienda o della scuola.

Firma digitale
Procedura che garantisce l'integrità e l'autenticità di un documento informatico, in analogia con la firma autografa.

Flaming
"Fiammata" è il comportamento di botta e risposta con toni violenti, in crescendo, via *e-mail* o in un *forum.*

Hacker
Il termine significa "esperto di informatica" e indica chi ha molta esperienza nel campo e riesce anche a inserirsi in computer e reti, a scopo conoscitivo e non sempre malevolo.

Malware
Programmi che compiono attività illecite all'insaputa dell'utente.

Netiquette
Insieme di regole di buona educazione nelle comunicazioni in rete (*e-mail*, *forum*, gruppi).

Netizen
"Cittadino della rete" da *network citizen.*

Newbie
Neologismo gergale: un nuovo utente della rete, navigatore alle prime armi.
Nickname
Nome fittizio (nomignolo) scelto al posto del proprio nome per accedere a risorse in rete senza svelare la propria identità.
Peer to peer o P2P
Sistema di condivisione di documenti, musica e film tra *computer* personali: eMule, Morpheus, Azureus sono alcuni dei *software* per attivare una rete P2P.
Popup
"Saltar su". Indica le finestre che si aprono nel *browser* in modo automatico, di solito per pubblicità.
Ripper
"Squartatore". Un programma che acquisisce i dati da CD musicale o DVD video, anche protetto da copia, e li trasferisce sul disco fisso, per un'eventuale conversione e modifica o per copia abitualmente illegale.
Spam
Messaggi di posta elettronica non richiesti, contenenti riferimenti a siti di vendita di prodotti, generalmente fasulli o legati a truffe.
Spyware
Programma invisibile che cattura informazioni sulla navigazione dell'utente normalmente a fini pubblicitari. È analogo al "cavallo di Troia".
Trojan
Cavallo di Troia.
URL
L'indirizzo della pagina *web* che vogliamo consultare. Si scrive nel *browser*.
Warez
Neologismo usato per individuare *software* scaricabili abusivamente e illegalmente dalla Rete.
Wiki
Sistema di pubblicazione di testi che permette a più persone di intervenire per creare un documento in collaborazione. Può essere ristretto solo ad alcuni autorizzati, oppure aperto a chiunque. Un'applicazione è la Wikipedia, enciclopedia su Internet scritta da chiunque.

Alcune fonti di questa guida

- www.apprendereinrete.it di Microsoft (con la collaborazione di Giunti labs) contiene risorse utili per i docenti di scuole secondarie
- www.tiseiconnesso.it è a cura del Ministero dello Sviluppo Economico - Comunicazioni e Save the children
- www.poliziadistato.it/pds/informatica contiene consigli della Polizia delle Comunicazioni
- www.ragazzieweb.it contiene filmati per i ragazzi sui rischi di Internet, videointerviste a specialisti e corsi su Internet e sulla sicurezza informatica per i genitori e i docenti
- www.genitori.it è il sito del Moige – Movimento Italiano Genitori che agisce per la tutela dei diritti dei genitori e dei minori nella vita sociale
- www.ilfiltro.it/difesa raccoglie un elenco di programmi e di documenti utili per la difesa dei minori (e degli adulti) dai rischi di Internet
- www.crudele.it/affidabilita sono sedici domande per imparare a valutare l'affidabilità, attendibilità e credibilità di un sito *web*
- www.crudele.it/prudenza contiene consigli per proteggere i propri dati e tutelare i propri clienti e utenti nell'uso di tecnologie informatiche