di Manlio Cammarata

«La peste della libertà»

LA CENSURA SU INTERNET UN PERICOLO MORTALE

Abbiamo sempre considerato Internet come il simbolo e lo strumento della libertà di comunicare. Abbiamo detto che è tecnicamente impossibile limitare il flusso delle informazioni, imporre censure, vietare l'accesso. Ma forse non è vero, come si può capire scorrendo alcune pagine del Web.

«Censorship», censura: questa parola ricorre sempre più spesso nei discorsi sul futuro di Internet. Un acceso dibattito si è aperto nel '95, quando negli USA è stato presentato il «Computer Decency Act» (CDA), poi recepito nel «Telecommunication Act of 1996», e qualcuno ha tirato un sospiro di sollievo il 12 luglio, quando una corte federale della Pennsylvania ha bloccato, provvisoriamente, le disposizioni censorie. La complessa motivazione della decisione è fondata su due punti essenziali: censurare i contenuti di Internet è impossibile, qualsiasi censura viola la libertà di espressione sancita dal Primo emendamento della Costituzione americana.

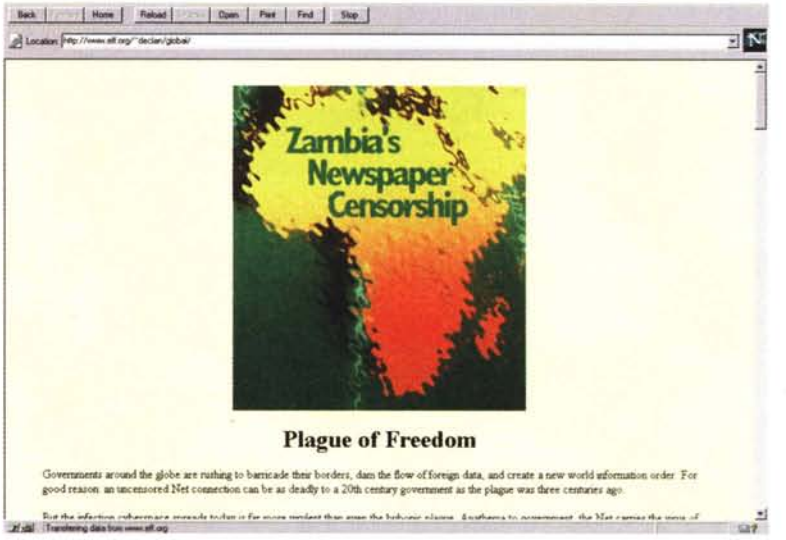
Censurare Internet è impossibile: ma è vero? Qualcuno ha iniziato seriamente a farlo: la Repubblica popolare cinese ha bloccato l'accesso a un centinaio di siti «pericolosi», il governo di Singapore ha classificato le informazioni e ha stabilito una serie di categorie vietate. Un giudice tedesco ha imposto a Compuserve di bloccare l'accesso a siti che propongono contenuti pornografici, e sono solo alcuni tra gli episodi più noti. Ma c'è un fatto ancora più grave, che è sfuggito a molti: la conferenza del G7 sul terrorismo, che si è tenuta a Parigi il 30 luglio '96, ha invitato tutti gli stati a vigilare sul fatto che i terroristi si servono delle reti telematiche e a prevedere limitazioni all'uso della crittografia, per prevenire atti terroristici o investigare «proteggendo la riservatezza delle comunicazioni legittime».

Censura e divieto della crittografia sono cose diverse, ma presentano un denominatore comune: il rischio di chiudere la stagione di Internet come strumento di libera espressione del pensiero, di conoscenza, di diffusione della cultura, di legittime attività economiche. Per quanto riguarda i «filtri», cioè la censura, si è sempre sostenuto che la natura stessa della Rete rende impossibile forme efficaci di controllo, ma questo è vero solo in parte. Perché, come spiega Alberto Berretti nell'intervista pubblicata più avanti, è sempre possibile aggirare gli ostacoli tecnici. Ma queste possibilità non sono alla portata di tutti, occorrono competenze tecniche e collegamenti particolari con soggetti che operino all'esterno delle aree «chiuse», e questo significa che i divieti possono essere efficaci nei riguardi della massa degli utenti. Il problema del divieto della crittografia è diverso e richiede un approfondimento che rimandiamo ai prossimi paragrafi.

Ora è bene mettere a fuoco i termini del problema, naturalmente avendo sott'occhio l'oggetto del contendere, e cioè Internet. A chi voglia farsi un'idea più precisa delle diverse questioni consiglio una navigazione fino al sito **http://www.eff.org/~declan/global**. C'è un elenco impressionante di casi di censura su Internet, o di semplici proposte o tentativi per imporla: a parte gli esempi ben noti della Cina e di Singapore, ci sono informazioni da ogni parte del mondo, dagli Stati Uniti all'Australia, alla Corea, allo Zambia, al Sud America e al Medio Oriente. C'è da riflettere sulle notizie dall'Europa, in particolare da Gran Bretagna, Francia, Germania, Olanda, Svezia, Svizzera. Per fortuna l'Italia... nó, c'è anche l'Italia, con un *link* a un documento che si intitola: «Italian net-censorship necessary, says Simon Wiesenthal

Ctr». Ma il documento è inaccessibile (se qualcuno ne sa di più, o riesce ad acquisire il testo, farà cosa utile a tutti inviandolo alla mia casella e-mail: m.cammarata@mclink.it).

Dall'elenco e dalla lettura più o meno casuale di qualche pagina si ricava l'impressione che siano in atto in tutto il mondo tentativi più o meno convinti di mettere il bavaglio a Internet. È una situazione molto preoccupante, perché se la comunità internazionale riesce a mettersi d'accordo su una serie di misure minime di censura sui contenuti della Rete, la libertà di espressione finisce, e con essa la libertà di tutti gli individui.



La pagina della Electronic Frontier Foundation dedicata alla censura su Internet.

I contenuti pericolosi

Il pretesto per mettere sotto controllo la grande rete è la necessità di limitare la circolazione dei contenuti «pericolosi». Pericolosi per chi e perché? Questo è il primo punto.

Non c'è dubbio che su Internet passano informazioni che possono essere considerate «pericolose» sotto diversi e condivisibili punti di vista. È nota la presenza di siti e gruppi di discussione che è poco definire «indecenti», per non parlare del reale problema dei «pedofili telematici». Altrove sulla Rete si possono trovare informazioni utili per compiere atti di terrorismo, o addirittura incitazioni a metterli in atto; soprattutto è noto (anche se non evidente!) che la malavita organizzata si serve ampiamente della posta elettronica per combinare loschi affari. Si aggiunga che su Internet circolano messaggi di forte contenuto razzista che, fatta salva la libertà di espressione, è bene non mettere alla portata dei giovani. Le menti dei ragazzi, facilmente influenzabili perché non hanno ancora sviluppato un sufficiente spirito critico, devono essere protette da suggestioni di violenza e di odio. Forse è il caso di ricordare che gli stessi contenuti si possono trovare nelle librerie e nelle edicole, ma che nessuno pensa di impedire l'attività di librai e giornalai...

Bisogna però sottolineare che questi aspetti costituiscono una parte molto limitata dei contenuti della Rete. La notizia che «Internet è intasata dal sesso» (vedi il riquadro sulla Rai) è falsa e tendenziosa. Falsa perché, come si può dimostrare con facili ricerche, il sesso in generale non è molto presente sulla Rete, tendenziosa perché crea un facile, ingenuo consenso sulle proposte di censura.

Internet è veramente il luogo di perdizione che da più parti si descrive? Cerchiamo la risposta in una fonte al di sopra di ogni sospetto, il quotidiano cattolico *L'Avvenire*. Sul quale Marco Cobianchi ha scritto l'8 febbraio scorso: *Se siete abbonati a Internet o se avete intenzione di farlo, sappiate che avete molte più probabilità di imbattervi in un sito religioso di quante non ne avete di transitare su uno sessuale. Eppure è così. Esattamente il 21,7% in più, che poi è la differenza tra la quantità di risorse che rispondono alla parola chiave* church *rispetto a quelle che hanno al loro interno la parola* sex. *La scoperta è tanto più interessante quanto facile da compiere: basta usare uno di quegli strumenti che, dopo aver inserito una parola chiave, vengono sguinzagliati per la rete. Cinque secondi ed ecco elencate in video tutte le risorse che corrispondono alla parola data...*

... in entrambe le sedute dell'esperimento, il 31 gennaio e il 4 febbraio, church *batte ampiamente* sex. *L'ultimo giorno del mese scorso risultavano presenti in Internet ben 4.782 pagine Web rispondenti a church rispetto alle 4.191 di sex...*

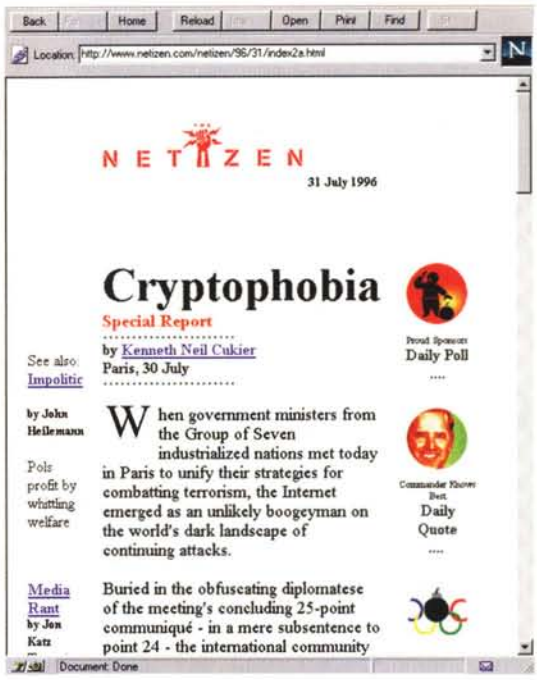
Ho personalmente ripetuto l'indagine il 15 agosto scorso, usando il motore di ricerca «AltaVista». Che, quel giorno, annunciava la possibilità di accesso a 30 milioni di pagine su 275.600 server. Ecco il risultato: la parola «church» era presente 1.210.055 volte in circa 300.000 documenti; la parola «sex» 1.964.316 volte, ma solo in circa 200.000 documenti. «Il sesso su Internet» è presente dunque in percentuale modesta, in confronto alla quantità di informazioni reperibili sulla Rete, e non è facile trovarlo. Lo ha confermato tempo fa Umberto Eco in una celebre «Bustina di minerva» su l'*Espresso* (non trovo più la divertente pagina: qualcuno può inviarmene una fotocopia in redazione, o almeno indicarmi il numero della rivista nel quale fu pubblicata?).

Certo, il fatto che il sesso sia presente su Internet in misura modesta non basta a dire che il problema non esiste. Ci sono pagine e newsgroup il cui contenuto è palesemente inadatto ai bambini e bisogna fare qualcosa per evitare che essi ne vengano influenzati. Ma da qui alla censura dei siti che contengono «sesso» di distanza ne corre! Prima di tutto perché le rappresentazioni erotiche in un modo o nell'altro fanno parte della cultura di quasi tutte le società, poi perché anche l'erotismo audiovisivo può essere considerato un diritto, almeno per gli adulti e fino al punto in cui non offende altri individui. Ma soprattutto perché il concetto stesso di «censura» deve essere bandito dalle nazioni che si definiscono libere e democratiche. Molti potrebbero essere d'accordo nel met-

tere un lucchetto ad alto livello, valido per tutti, che chiuda l'accesso alla pornografia più turpe. Ma chi stabilisce il confine tra il lecito e l'illecito? Gli stessi contenuti possono essere considerati intollerabili da qualcuno, innocui o addirittura divertenti da qualcun altro. Come si può delegare a un organismo qualsivoglia il diritto di vietare questo o quel contenuto? La trappola è proprio qui: se si accetta che il principio che qualcuno decida che cosa può essere visto e che cosa no, è facile passare dal sesso alla politica, alla cultura, alla religione.

Ci sono modi diversi dalla censura per limitare l'accesso ai contenuti pericolosi. Essi sono fondati su meccanismi di autoregolamentazione e perfettamente applicabili su vasta scala, senza il ricorso a provvedimenti autoritari. Alcuni sono già disponibili: negli USA è possibile stipulare abbonamenti a Internet «per le famiglie» con fornitori che inibiscono l'accesso ai contenuti «indecenti»; nel *browser* «Internet Explorer» di Microsoft è prevista la possibilità di subordinare all'inserimento di una *password* l'accesso a determinate URL, che è quanto basta al «genitore medio» per proteggere l'innocenza di un «bambino medio». Presto dovrebbe diffondersi la «piattaforma per la selezione dei contenuti di Internet» della quale si parla nel riquadro in queste pagine.

Ma la censura sui contenuti pericolosi fornisce ai governi uno strumento potentissimo per controllare l'uso della Rete, come dimostra il caso di Singapore.



Dalla rivista «Hotwired» le informazioni sulle proposte di censura in Francia.

I benefici «imbrigliati»

La Cina ha bloccato l'accesso a un centinaio di siti Internet «sospetti di portare inquinamento spirituale», come riferisce il Wall Street Journal del 5 settembre scorso (tutte le informazioni riportate in queste pagine sono ricavate da Internet). Il punto è che tra questi fornitori di informazioni, inquinanti secondo le autorità cinesi, c'è lo stesso Wall Street Journal, c'è la CNN, ci sono altre organizzazioni che a noi sembrano tutt'altro che pericolose. Ma è chiaro che il vero inquinamento, per i paesi retti da regimi autoritari, è dato dall'informazione libera, da quella che la Electronic Frontier Foundation definisce *Plague of Freedom*, la «peste della libertà». Ma la censura cinese appare rozza e ingenua di fronte alla regolamentazione introdotta a Singapore: articolata, logica e ipocrita ai limiti dell'immaginabile.

La legge di Singapore ricorda sotto alcuni aspetti il nostro decreto legislativo 103/95 e i disegni di legge sulle telecomunicazioni all'esame delle Camere, perché stabilisce un regime di autorizzazioni (*license*) per i fornitori di Internet. Ma è molto più informata e precisa, perché distingue tra fornitori di accessi e fornitori di informazioni. I primi (Internet Access Service Providers) sono distinti per categorie, come i rivenditori di accessi (i nostri POP?) localizzati e non localizzati, mentre si considera fornitore di informazioni (Internet Content Provider) ogni persona che fornisce informazioni sul World Wide Web, compresi gli editori e gli amministratori (intesi in senso commerciale) di server Web.

Tutti i fornitori di accessi devono registrarsi (il nostro regime dichiatorio) presso l'autorità competente, che si chiama SBA, Singapore Broadcasting Authority; chi vuole cercare affinità con la «Autorità per le garanzie delle comunicazioni», che sta per essere varata dal nostro Parlamento, è libero di farlo, ma con le dovute distinzioni. A Singapore la registrazione non è richiesta per i fornitori di contenuti, a meno che non siano partiti politici, o persone o gruppi impegnati in discussioni politiche o religiose che riguardano la nazione, oppure giornali telematici che intendano trovare abbonati tra i cittadini di Singapore. Naturalmente è necessario pagare qualche tassa, in funzione del numero degli abbonati. Ci sono poi altri servizi che possono essere autorizzati: audiotex, videotex e altri, compresi i BBS.

Seguono una serie di prescrizioni sui termini per la registrazione, e in molti punti sembra di leggere le norme nostrane, con ovvie differenze per quanto riguarda i contenuti, ma con fondamenti tecnici precisi, che dimostrano come il legislatore asiatico sia molto più competente del nostro.

Il rapporto della Electronic Frontier Foundation riferisce che la SBA «riconosce che è impossibile regolare completamente Internet» e che «il successo della regolamentazione di Internet dipende moltissimo dall'autoregolamentazione dell'industria e dall'azione della comunità». Ma, ad ogni buon conto, emana una serie di norme precise. L'allegato alla regolamentazione, annunciata l'11 luglio 1996, afferma che *Internet è un prezioso*

strumento di comunicazione e di ricerca. L'Autorità continuerà a promuovere il suo uso nella diffusione dell'informazione e nello scambio delle idee. Prosegue il testo: *È dovere dell'Autorità salvaguardare l'interesse nazionale di Singapore e assicurare che i benefici di Internet siano imbrigliati per il bene generale della nostra società* («imbrigliato» è il significato letterale di «harnessed»; la traduzione dal testo inglese è mia e chiedo scusa se c'è qualche imprecisione). *L'Autorità crede che regolare Internet possa aiutare lo sviluppo di una sana cultura di Internet dove l'uso responsabile degli aspetti positivi di Internet sia la norma. A tutti i fornitori autorizzati di servizi e di*

Sergio Zavoli contro Internet: la Rai fa la sua parte

Più volte in queste pagine abbiamo criticato il modo in cui i mass media parlano dei temi della società dell'informazione e di Internet in particolare, con la continua pubblicazione di articoli che mettono in risalto gli aspetti negativi della Rete. Mentre manca quasi del tutto la divulgazione dei tanti argomenti che potrebbero aiutare a superare il diffuso analfabetismo tecnologico che contraddistingue ancora il nostro paese.

Questo atteggiamento è particolarmente grave per un mezzo come la televisione, capace di un fortissimo potere di persuasione, e che più di ogni altro potrebbe svolgere una corretta azione informativa ed educativa. Ma sembra che a Viale Mazzini non abbiano ancora le idee molto chiare sulle implicazioni che lo sviluppo delle tecnologie avrà sulla stessa struttura radiotelevisiva di Stato e sulla opportunità di «preparare» gli utenti ai nuovi schemi dell'informazione.

C'è una sola trasmissione della Rai che si occupa in qualche modo dei nuovi media: si chiama Media/Mente e va in onda il mercoledì a notte fonda su Raiuno, con una breve «finestra» mattutina ogni giorno su Raitre. Media/Mente è un programma interessante dal punto di vista formale: costruito su un abile e veloce gioco di montaggi digitali, con un linguaggio visivo raffinato e molto moderno, affida alla indiscutibile bravura di Carlo Massarini una serie di suggestioni assolutamente superficiali, tese più a stupire che a informare. A volte Massarini snocciola a velocità supersonica raffazzonate e imprecise spiegazioni tecniche, assolutamente incomprensibili, in altri momenti va in estasi di fronte a situazioni che appaiono scontate a chiunque abbia una minima esperienza della Rete. In molti casi è evidente che parla di cose delle quali non ha una conoscenza diretta, e gli stessi testi sembrano preparati da qualcuno che i nuovi media li conosce vagamente, per sentito dire. Sfuggono del tutto agli autori del programma tanti fenomeni di attualità che potrebbero aiutare il pubblico a capire che cosa succede nel mondo delle tecnologie dell'informazione, fenomeni che non riguardano solo Internet e i compact disc, ma anche (chi l'avrebbe mai detto?) la stessa televisione. Si aggiunga che Media/Mente, col suo linguaggio spigliato, si presenta come un programma per i ragazzi: ma allora perché lo mandano in onda alle ore piccole? Insomma, un'occasione perduta per quella diffusione culturale che dovrebbe essere uno dei compiti principali del servizio pubblico televisivo.

Un'altra opportunità sprecata è la serie di episodi «Interset - cronache reali dal mondo virtuale», in onda su Raitre nella seconda serata del sabato. Filmati di un'ora, una sciatta «fiction» che simula improbabili «news», fondata sui luoghi comuni di Internet: l'amore in rete, i pirati telematici e altre banalità. Tutto cucito da una sceneggiatura che ruota intorno alla figura di un cronista intronato che gira e fa domande, senza capire un'acca di quello che gli raccontano personaggi stralunati, tanto più incredibili quanto più vengono presentati come reali.

Tra fanta-cronaca e finta cronaca, «Interset» si può ben inserire nel filone «anti-Internet» di molta stampa, quella che cerca di esorcizzare il progresso attraverso la diffamazione, per mantenere un assetto destinato prima o poi a crollare.

È una strategia premeditata o solo il frutto di incompetenza e improvvisazione? Il dubbio sorge di fronte a uscite come quella del TG2 del 21 agosto: sono i giorni in cui i giornali danno grande risalto ai fatti di Marcinelle, in Belgio, dove è stata scoperta una coppia di maniaci sessuali assassini. Fra le altre informazioni viene data quella dell'uso di Internet per i turpi traffici delle organizzazioni dei pedofili. Notizia vecchia, che meriterebbe una frase o poco più, per completezza di informazione. Ma la cosa viene «pompata» in un apposito servizio, nel quale si afferma testualmente che «Internet è intasata dai siti dedicati al sesso». Informazione falsa e tendenziosa. Falsa perché il sesso rappresenta una piccolissima parte dei contenuti della Rete (che non è affatto intasata), tendenziosa perché, ancora una volta, contribuisce a diffondere una visione negativa dei nuovi mezzi di informazione.

Ma c'è di più: alla notizia segue un commento, affidato nientedimeno che a Sergio Zavoli. Il celebre giornalista spara un moralistico pistolotto che, partendo dal principio che «Internet è intasata dal sesso» arriva a concludere che il «villaggio globale» è in realtà un «villaggio tribale». Naturalmente il maestro del giornalismo televisivo, autore di programmi straordinari come «La notte della Repubblica», è libero di pensare quello che vuole di Internet e di tutto il resto. Ma, prima di apparire a pieno schermo per commentare una notizia, dovrebbe avvertire il dovere professionale di verificarla.

contenuti Internet è richiesto di uniformarsi a queste linee-guida sui contenuti e di soddisfare l'Autorità per aver assunto misure adeguate a soddisfare queste richieste. Gentile, no?

Le linee-guida elencano quindi i contenuti non permessi *(The following Internet contents should not be allowed).* Sono previste tre categorie, che riguardano la pubblica sicurezza e la difesa nazionale, l'armonia razziale e religiosa e la morale pubblica. Nella prima rientrano i contenuti che minano la fiducia nell'amministrazione della giustizia, o possono gettare allarme nella popolazione, o che possono suscitare odio o disaffezione verso il governo. Nella seconda categoria sono compresi i contenuti che denigrano o prendono in giro gruppi razziali o religiosi, che suscitano odio o risentimento razziale e religioso e che promuovono deviazioni religiose o pratiche occulte, come il satanismo. Per quanto riguarda la morale pubblica, sono ovviamente vietate le rappresentazioni pornografiche o in altro modo oscene, la diffusione di permessivismo e promiscuità, oltre al grossolano sfruttamento di violenza, nudità, sesso e orrore; infine sono vietati i contenuti che descrivono o propagandano perversioni sessuali come l'omosessualità e la pedofilia.

Ma come si fa ad assicurare il rispetto di questi divieti? È semplice: ogni fornitore di Internet non deve fare altro che programmare i propri router per filtrare i collegamenti agli IP Address che possono presentare contenuti che «should not be allowed». I testi che ho letto non parlano delle pene previste per chi non si adegua alle «richieste» della SBA, ma da quel che si dice della giustizia di Singapore dovrebbero essere molto dissuasive.

Il pasticcio della crittografia

Ma Singapore non è una nazione democratica. Noi, per fortuna, siamo in Italia, un paese in cui Internet è così libera che il legislatore non la prende nemmeno in considerazione. Un paese in cui vige una norma che dice: *Nella prestazione dei servizi di telecomunicazioni non sono ammesse restrizioni relative al trattamento dei segnali prima della loro trasmissione sulla rete pubblica o dopo la loro ricezione, diverse da quelle occorrenti per la salvaguardia delle esigenze connesse all'ordine pubblico, alla sicurezza pubblica ed alla difesa nazionale.* Norma presa tale e quale dalle disposizioni dell'Unione Europea (direttiva 90/388) che significa semplicemente che non si può vietare la crittografia. E qui affrontiamo un argomento sul quale i governi si esercitano in diatribe inutili quanto pericolose.

PICS, il controllo senza censura

Il problema è semplice da descrivere, ma sembra complicato da risolvere: su Internet si trovano contenuti il cui accesso, per un motivo o per l'altro, alcuni soggetti vorrebbero precludere ad altri soggetti. È il caso di alcuni governi che ritengono di dover proteggere i cittadini dai contenuti «inquinanti», dei genitori che cercano di proteggere i figli dalla pornografia, delle aziende che vogliono evitare che i dipendenti perdano tempo girovagando per la rete. La soluzione è più semplice di quanto possa apparire a prima vista: bastano un'etichetta che indichi il contenuto delle pagine e un software che blocchi il collegamento in presenza di determinate etichette. Questo meccanismo è già stato adottato in forme diverse, ma dall'inizio di quest'anno c'è anche uno standard di fatto, adottato sia dai più grandi fornitori di informazioni (CompuServe, America On Line, Prodigy ecc.), sia dalle case che producono i browser, come Microsoft e Netscape.

Il sistema si chiama PICS (Platform for Internet Content Selection). Le etichette possono essere introdotte da diverse organizzazioni, a seconda dei contenuti che si vogliono filtrare, e il superamento del blocco può essere subordinato all'inserimento di una password (in questo modo solo chi conosce la password può accedere a certe pagine o a certi siti). Ma il filtro di PICS può essere adottato anche dagli Internet Provider, che in questo modo sono in grado di offrire alle famiglie abbonamenti garantiti contro i contenuti «indecenti», con buona pace di tutti quelli che vorrebbero togliere da Internet (cioè dal mondo) ogni informazione sul sesso.

Il sistema PICS dovrebbe diffondersi in tempi brevi su tutta la Rete, anche perché i fornitori di informazioni che non lo adottassero si troverebbero ben presto ai margini del mercato.

Così non si potrà più dire che «Internet è un rischio per i bambini» o altre cose del genere, e quindi nessuno potrà invocare in buona fede le forbici della censura «alla fonte». Naturalmente sarà necessario che qualcuno attivi i filtri, e molti genitori potrebbero trovarsi in difficoltà. Ma anche per questo c'è la soluzione pronta: diverse organizzazioni, a partire dall'UNICEF, distribuiranno pacchetti «preconfezionati» per la censura familiare.

C'è un solo «ma»: il sistema potrebbe essere usato «dall'alto» e rendere più facili le censure governative. Basterebbe imporre a tutti i fornitori di accessi di una nazione l'uso del PICS per determinati contenuti, e addio libertà dell'informazione.

C'è solo da sperare che qualcuno inventi un software contro le dittature.

Le informazioni su PICS, il sistema di «controllo senza censura», sono alla URL http://www.w3.org/pub/WWW/PICS.

Tutti sono d'accordo sul fatto che la crittografia è l'unico sistema possibile per la riservatezza delle informazioni trasmesse via Internet. Quando si parla di riservatezza delle informazioni non ci si riferisce solo alla corrispondenza privata, ma anche e soprattutto a quella commerciale, per la quale la violazione di un segreto può comportare conseguenze catastrofiche. La crittografia è anche alla base di tutti i sistemi di pagamento telematici: vietarla significherebbe uccidere il commercio in rete, un settore sempre più importante per l'economia mondiale. Ma, dicono alcuni, la crittografia protegge i traffici della malavita, del terrorismo, dei pedofili e di quanti altri hanno la coscienza sporca: quindi vietiamo la crittografia.

Soluzione inutile e dannosa, prima di tutto perché i mascalzoni smetterebbero di usare la posta elettronica e troverebbero altri sistemi per lo scambio di informazioni, poi perché si metterebbe in pericolo la riservatezza della corrispondenza privata e commerciale. Ecco che alcuni suggeriscono di adottare una via di mezzo: consentiamo l'uso della crittografia, ma a patto che le «chiavi» siano consegnate a un'apposita autorità, che le metta a disposizione della giustizia in determinati casi. Apparentemente è una soluzione equilibrata, e in Francia è stata recentemente inserita nella legge di riforma delle telecomunicazioni. Ma è subito finita davanti alla Corte Costituzionale, insieme a una serie di vincoli posti agli Internet Provider per i contenuti «pericolosi». Non va dimenticato, in questo quadro, il tentativo del governo statunitense per imporre l'inserimento in tutti i sistemi on-line di un microcircuito, il «Clipper chip», che consenta alle autorità di decrittare qualsiasi messaggio. La proposta è stata seppellita da un coro di proteste, ma è discutibile il principio stesso di un Grande Fratello decifratore, sotto le spoglie di un organismo pubblico che detiene tutti i codici crittografici

A ben guardare, sostenitori di questa soluzione o sono nati ieri, o sono in malafede. Chi garantisce che, in un paese come l'Italia, l'archivio delle chiavi di decrittazione resti realmente segreto? Il nostro Ministero dell'Interno, che dispone di una banca di informazioni personali che nessuno riesce a controllare né in entrata né in uscita? I Palazzi di Giustizia, in cui basta «segretare» un verbale per vederlo il giorno dopo su tutti i giornali? Gli americani della CIA o gli inglesi dell'MI5, i cui rapporti riservatissimi vengono frequentemente diffusi come se fossero agenzie di stampa?

Il rischio del «key escrow», cioè delle chiavi affidate a terzi, è troppo alto. Se gli investigatori non riescono a leggere la corrispondenza illegale, possono ricorrere ad altri sistemi, come dimostrano le cronache più recenti (tu usi i telefonini GSM svizzeri, che io non posso ascoltare? E io ti faccio l'intercettazione ambientale).

Tra l'informazione tradizionale e i nuovi mezzi di comunicazione ci sono differenze notevoli. Ma i diritti dei cittadini sono sempre gli stessi, e se non si può incriminare un edicolante per i contenuti dei giornali, così non si deve limitare la libertà di un fornitore di accessi a Internet per i contenuti delle pagine Web. E vietare la crittografia nella corrispondenza elettronica è come vietare le buste nella posta tradizionale: *La libertà e la segretezza della corrispondenza e di ogni altra forma di comunicazione sono inviolabili,* dice l'articolo 15 della nostra Costituzione.

«Privacy International» è un'altra organizzazione per la protezione dei diritti dei cittadini in rete (http://www.privacy.org).

La soluzione tecnologica

Ci sono altri sistemi per prevenire e reprimere i reati che possono essere commessi sfruttando i mezzi telematici, sistemi che devono essere adottati e imposti da tutti i paesi. Il primo è l'identificazione degli utenti: ci deve essere la certezza dell'identità di chi stipula un abbonamento a un servizio telematico ed è quindi responsabile dell'uso delle chiavi di accesso. Questo non significa vietare l'anonimato telematico: chiunque deve avere il diritto di usare uno pseudonimo (purché non generi equivoci) e di assumere un'identità virtuale.

Ma il gestore del servizio deve essere obbligato a mantenere segreta l'identità e altri dati di un abbonato che voglia mantenere un anonimato più o meno stretto, tranne che in seguito a un provvedimento motivato dell'autorità giudiziaria. Il secondo accorgimento, strettamente legato al primo, è la tenuta di registri digitali automatici (log) di tutti gli accessi, che consentano di risalire all'autore di collegamenti o di messaggi illegittimi.

A mio avviso queste due precauzioni, identificazione degli abbonati e registrazione dei collegamenti, dovrebbero essere rese obbligatorie da precise disposizioni di legge. Ci sono però diffuse e motivate resistenze all'introduzione di norme di questo tipo, che di fatto limitano in una certa misura la libertà di comunicare. Si dice che la documentazione dell'identità e dei collegamenti non offre la sicurezza che l'autore di un certo atto illecito sia proprio il soggetto indicato dalle registrazioni, e questo è vero. Ma è lo stesso discorso della targa dell'automobile: essa fornisce una «certezza legale», che può essere smentita dalla prova contraria.

Se viene rilevata la targa di un'auto che commette una certa infrazione, il proprietario può dimostrare che in quel momento non la guidava lui.

E nessuna persona di buon senso ha mai proposto di abolire le targhe delle automobili, per il fatto che limitano la «privacy» del proprietario!

È una limitazione universalmente accettata, perché assicura alla collettività la protezione contro i «pirati della strada» e la repressione dei reati che possono essere commessi con l'uso di un'automobile. Nello stesso modo si deve accettare l'anonimato «limitato» sulle reti telematiche, perché esso protegge in qualche misura dalla criminalità comune e tecnologica. E, soprattutto, perché spunta le armi di coloro che vorrebbero imporre norme ancora più limitative, come il divieto della crittografia o le «escrow key», che sono praticamente la stessa cosa.

Ora riassumiano i fatti. Primo: sulle reti passano informazioni illecite e pericolose, protette dall'anonimato e dalla crittografia; secondo: vietare la crittografia è inutile e dannoso, perché i malfattori possono trovare altre strade per comunicare e si colpisce la riservatezza delle comunicazioni legittime. Tra i due mali si deve scegliere una soluzione intermedia, che consiste nel favorire la prevenzione e la repressione del crimine con strumenti che limitano solo in parte la libertà di comunicare, come il divieto di quello che possiamo chiamare «anonimato assoluto» e l'obbligo della documentazione dei collegamenti.

Sono misure che rendono più complicata e onerosa l'attività dei gestori dei sistemi telematici, che in qualche caso sono contrari all'introduzione di norme di questo tipo. Esse però potrebbero rivelarsi estremamente vantaggiose se fossero accompagnate da una previsione legislativa di questo tipo: quando un sistema telematico è coinvolto in fatti di rilevanza penale attribuibile a terzi, esso non può essere sottoposto a sequestro se il responsabile consegna all'autorità giudiziaria tutta la documentazione utile a identificare l'autore degli illeciti. Documentazione che, è ovvio, deve presentare certi requisiti di attendibilità, che la possano far ritenere «certa» fino a prova contraria (per chi è all'oscuro dei meccanismi giuridici: un documento può costituire una prova a favore o contro chi lo ha redatto, a seconda dei casi; ma se un documento è in qualche modo «certificato» il suo contenuto si assume che sia «vero», a meno che qualcuno non riesca a provare che è falso). Insomma, l'onere della documentazione potrebbe proteggere i sistemi telematici dal rischio di interruzioni del servizio, che potrebbero essere disposte dalla magistratura nel corso di indagini su fatti illeciti.

Tutto questo porta a un'altra serie di considerazioni: è necessario che l'autorità giudiziaria e le forze di polizia siano messe in grado di perseguire i reati tecnologici con la massima efficacia possibile. La recente istituzione della Polizia delle telecomunicazioni, composta da specialisti molto preparati e dotata di attrezzature adeguate, è un passo avanti, ma non basta. È necessario non solo estendere la preparazione specifica a settori sempre più ampi delle forze dell'ordine, ma soprattutto stabilire che ogni segnalazione di fatti illeciti che coinvolgano sistemi tecnologici debba essere immediatamente girata ai reparti specializzati, e che le indagini vengano sistematicamente coordinate da sostituti procuratori dotati di una preparazione specifica. Anche le norme di procedura devono essere adeguate alla realtà tecnologica e consentire agli inquirenti di mettere tempestivamente in atto misure efficaci per l'indentificazione dei responsabili di azioni cirminali.

«Colpire nel mucchio», come purtroppo è stato fatto qualche volta in passato, non serve a perseguire il crimine in modo efficace, ma solo a limitare la libertà degli utenti onesti. Quella libertà che può essere messa in pericolo da una legislazione repressiva, dovuta nei fatti all'incapacità di perseguire efficacemente la criminalità tecnologica.

Gli anticorpi di Internet

Lo stesso discorso si ripropone, in termini solo apparentemente diversi, per quanto riguarda i contenuti «pericolosi» di Internet. Se la protezione dal crimine tecnologico non deve limitare il diritto alla riservatezza di ogni utente, la difesa della «morale» non deve colpire la libertà di manifestazione del pensiero. In ambedue i campi è però indispensabile accettare qualche limitazione, purché sia realmente utile a combattere gli aspetti negativi o degenerativi della libertà di comunicare.

Qui può essere opportuno accennare a un discorso di ordine generale sulla natura delle tecnologie. Ci sono persone che nutrono una sconfinata fiducia negli aspetti positivi del progresso tecnologico, mentre altri sottolineano soprattutto gli aspetti negativi e pericolosi per un «sano» sviluppo della società.

Tra queste due posizioni si colloca una terza, e forse più pericolosa, visione, che si riassume

L'ho letto su Internet...

Qualcuno potrà sembrare strano, ma il sistema migliore per avere informazioni su Internet è proprio andarle a cercare su Internet! Così si può anche verificare quanto sia falsa la storia del «caos informativo» della Rete e come sia relativamente semplice trovare quello che di volta in volta ci interessa.

Per realizzare questo servizio sul controllo di Internet da parte dei vari governi sono partito con un'indagine su AltaVista, il grande «motore di ricerca» realizzato dalla Digital, con le parole chiave «Singapore», «Internet» e «censorship» (censura). È bastato scorrere le prime pagine di link per identificare due fonti sicure: l'Internet Society e l'Electronic Frontier Foundation (potevo pensarci prima!). Sul primo sito c'è una storia dettagliata di come sia nata la censura di Internet a Singapore (http://info.isoc.org/HMP/PAPER/132/abst.html è il documento di partenza), da un altro link sono risalito a una pagina della EFF intitolata «Plague of Freedom» (http://www.eff.org/~declan/global) che potrebbe avere lo slogan «tutto quello che vorreste sapere sul controllo di Internet a livello mondiale». Da qui si può partire con ricerche che coprono, purtroppo, tutto il globo terrestre. Mi è bastato seguire una piccola parte delle centinaia di link sull'argomento per trovare tutte le informazioni riportate in questo articolo e tante altre che lo spazio impedisce di riportare.

nella formula della «neutralità delle tecnologie»: secondo questa teoria, l'innovazione in sé non è né «buona» né «cattiva», dipende dall'uso che se ne fa.

Questa affermazione non può essere accettata. L'innovazione tecnologica, frutto del progresso della scienza, è sempre positiva, perché estende le conoscenze dell'uomo e allarga le possibilità di migliorare la qualità della vita di tutti gli individui. Ma può essere usata male, questo è il punto.

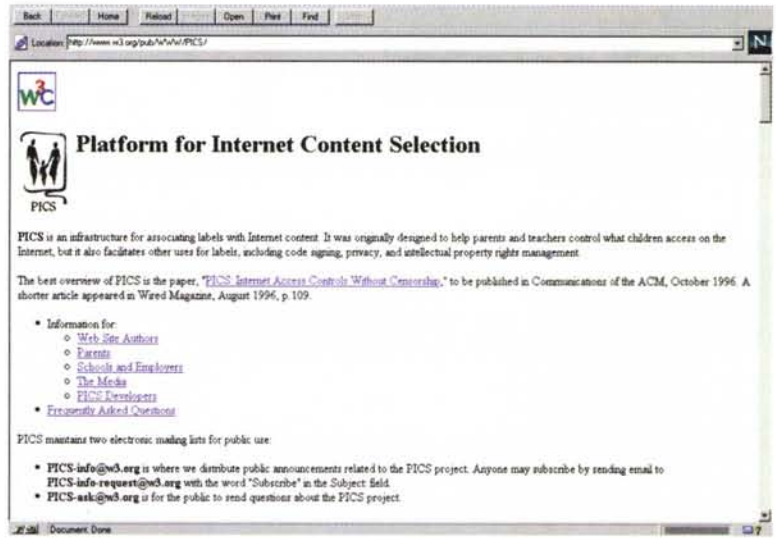
Anche il governo di Singapore riconosce i vantaggi sociali della diffusione di Internet, ma si preoccupa degli effetti negativi che possono essere determinati da certi contenuti.

È una questione di punti di vista: nelle società democratiche si ritiene, almeno in linea di principio, che la libertà di espressione sia un bene meritevole di una tutela più ampia di quella che deve essere accordata a particolari visioni morali o etiche; altrove la tutela di determinati valori è considerata più importante di una generale libertà di diffusione delle idee e di accesso alle informazioni. La differenza sostanziale è nel fatto che nei paesi democratici la linea di confine viene stabilita attraverso un processo che coinvolge tutti i cittadini, mentre negli altri è stabilita con meccanismi di tipo autoritario. I paesi dell'Occidente si riconoscono nella prima categoria, quindi in queste nazioni non possono essere accettate regole «dall'alto» che stabiliscano limiti alla libertà di comunicazione, fino al punto in cui l'abuso di questa libertà non produca un danno sociale.

Attenzione: il confine tra l'uso e l'abuso della libertà non può essere determinato a priori, ma si rileva proprio nel momento il cui si produce o si rischia di produrre un danno. Se si accetta il principio che determinati contenuti possono creare un danno sociale, è necessario intervenire ponendo qualche limite.

Dunque, se le rappresentazioni di deviazioni sessuali, l'incitamento all'odio razziale o la diffusione indiscriminata e continua di contenuti violenti possono causare seri problemi nello sviluppo dei minori, o produrre turbamenti psicologici o comportamentali in un numero rilevante di individui, è bene introdurre regole sulla diffusione e sull'accesso a queste informazioni. Quali regole?

Ritorniamo al discorso sull'uso delle tecnologie: se esse sono impiegate «bene», possono servire anche a risolvere questi problemi. Questo assunto può essere dimostrato prima di tutto nel caso delle trasmissioni televisive, perché la possibilità di trasmissioni in codice «ad accesso condizionato» permette ai genitori di inibire ai figli la visione di trasmissioni pornografiche. Anche nel caso di Internet è già disponibile la soluzione «educativa»: si possono inserire contrassegni digitali che facciano scattare una censura volontaria, sia al livello del distributore, sia a quello dell'utente. È una tecnologia già disponibile e in fase di introduzione generalizzata. Basta inserire nei programmi di ricerca delle informazioni poche righe di codice che riconoscano questi contrassegni e richiedano l'inserimento di una «password» prima di rendere accessibili i contenuti pericolosi. Questi meccanismi possono anche essere utilizzati dai fornitori di accessi, che possono offrire abbonamenti «puliti» a chi ne faccia richiesta. E possono essere utilizzati anche nel caso di accessi collettivi, nelle aziende come nelle scuole, dove è opportuno limitare l'uso di risorse collettive destinate ad usi particolari, come l'educazione o le attività lavorative.



PICS (Platform for Internet Content Selection) è il sistema per un controllo dei contenuti senza censura.

Dunque è possibile governare l'uso dei nuovi mezzi di comunicazione, in funzione di esigenze particolari e per particolari categorie di utenti, senza porre limiti generalizzati alla libertà di diffondere e di conoscere le informazioni. Insomma, non ci sono giustificazioni per introdurre alcuna forma di censura o di controllo diretto sui contenuti. Il compito dei governi e delle autorità preposte alla disciplina dei mezzi di comunicazione deve essere solo quello di prescrivere l'adozione delle misure limitative da parte dei soggetti interessati: in pratica, basta imporre l'apposizione dei «contrassegni» ai fornitori di informazioni e dei filtri ai produttori dei software di accesso alle informazioni stesse. Tutto qui.

È necessario che tutti gli operatori dei nuovi media si rendano conto della necessità di adottare questi accorgimenti e che svolgano un'azione chiara e determinata nei confronti delle autorità e dei governi affinché i meccanismi di autoregolamentazione siano riconosciuti come validi e, se necessario, resi obbligatori. La difesa a oltranza di una generica e indiscriminata «libertà di comunicazione» può avere come risposta l'introduzione di divieti altrettanto generici e indiscriminati.

Internet possiede gli anticorpi per le sue stesse malattie. Essi devono essere attivati, perché se il male si diffonde possono rivelarsi necessarie medicine che presentano devastanti effetti collaterali. E se molti governi si mettono d'accordo per somministrare dosi massicce di queste medicine, il male della censura può uccidere l'organismo vitale della società dell'informazione.

È vero che in Internet c'è una sorta di anticorpo anche contro la censura, che la stessa natura tecnologica della Rete permette di conservare un minimo vitale di circolazione delle informazioni. Ma se dovremo arrivare a collegarci a Internet come i nostri padri e i nostri nonni ascoltavano Radio Londra nei tempi bui della guerra, vorrà dire che avremo perso il bene fondamentale della libertà.