Continua il dibattito sulla legge che manca

BBS e attività criminali

Superato l'impatto iniziale di «Fidobust», ermergono i problemi della regolamentazione giuridica dei sistemi telematici. Come conciliare sicurezza, libertà di comunicare e «privacy»

di Manlio Cammarata

Quale legge per la telematica?

La pausa estiva non ha fatto cadere l'attualità del dibattito sorto dopo l'operazione di polizia giudiziaria, iniziata l'11 maggio scorso, che ha portato alla chiusura di molti sistemi telematici in tutta Italia. Alla fine di giugno si sono svolti due convegni, uno a Roma e uno a Pesaro, nei quali sono stati raccolti contributi molto significativi per la futura regolamentazione del settore. In ambedue le occasioni Paolo Nuti ha espresso il nostro punto di vista e le nostre proposte, pubblicate sul numero scorso, nell'editoriale e in queste pagine di Informatica & Diritto.

Facciamo dunque il punto sullo stato della discussione, riportando le opinioni più significative emerse nelle due riunioni. Opinioni che in molti casi si sono rivelate concordi, mentre su alcuni aspetti di grande importanza sono emerse divergenze sostanziali, difficili da conciliare.

Guardie e ladri

Il convegno di Roma «Sistemi telematici e diritto» è stato organizzato a tempo di record da Agorà Telematica dopo l'operazione Fidobust.

Tra gli interventi più interessanti va ricordato quello di Alessandro Pansa, direttore del Nucleo centrale criminalità economica e informatica della Polizia di Stato. Pansa ha sottolineato un problema di estrema gravità: quello dei BBS impiegati come sistema di scambio di informazioni per la malavita organizzata. Un aspetto che altri relatori, nei due convegni, hanno preso seriamente in considerazione, e che può influire in misura notevole sulla futura regolamentazione del settore telematico. Quando si parla di sistemi di comunicazione utilizzati dalla grande criminalità, si pone inevitabilmente il problema dei controlli dei contenuti e delle intercettazioni dei flussi di dati, avvalorando le tesi di chi chiede norme che in qualche modo possono limitare la «libertà di modem» e la segretezza della corrispondenza. Da un dirigente della polizia, ogni giorno alle prese con gli aspetti illegali della materia, ci si aspettano indicazioni severe e proposte autoritarie; invece Pansa ha fatto un discorso molto aperto, giungendo ad affermare che non si può imporre ai responsabili dei sistemi telematici il «tracciamento» completo dei collegamenti (come hanno dimostrato gli scarsi risultati ottenuti con l'obbligo imposto alle banche di documentare certe categorie di movimenti, per evitare il riciclaggio dei proventi del crimine).

Non condividiamo questo punto di vista, perché la documentazione che si richiederebbe ai sistemi telematici è molto diversa, e molto più semplice, di quella imposta alle banche. Si tratta di installare semplici procedure di «LOG», del tutto automatiche, che servono al gestore anche per tenere sotto controllo il funzionamento del sistema, oltre a costituire uno strumento indispensabile per scoprire tentativi di effrazione e altri usi impropri del servizio.

L'avvocato Giovanna Corrias Lucente ha svolto una dettagliata analisi giuridica dei reati telematici, sottolineando la difficoltà di attribuire al gestore del sistema la responsabilità dei comportamenti delittuosi degli abbonati. Perché si pos-

Il convegno di Roma del 27 giugno ha fatto il punto della situazione dopo l'operazione Fidobust.

Il convegno di Pesaro del 30 giugno. Nelle altre foto, alcuni dei partecipanti.

sa profilare la responsabilità penale del gestore, ha detto Corrias Lucente, devono emergere sia l'elemento materiale della condotta del reo, sia l'elemento psicologico del dolo. In altri termini è necessario che il gestore commetta volontariamente un'azione prevista dalla legge come reato, e questo non avviene quando un sistema telematico viene impiegato per attività illegali da persone esterne alla struttura. Sotto questo aspetto la responsabilità del sysop è diversa da quella del direttore responsabile di una pubblicazione, che risponde anche di negligenza o di omissione di controllo sul contenuto degli articoli. Invece è stata riconosciuta, ha ricordato l'avvocato, la non responsabilità del direttore per i contenuti degli annunci economici, che non possono essere controllati facilmente. «Occorre pertanto - ha concluso Corrias Lucente - che la normativa concernente la responsabilità del gestore di un BBS sia assistita, come avviene per la stampa, dalla riserva di legge di cui all'articolo 21 della Costituzione in ordine al sequestro, ma preveda precisi limiti di intervento da parte del potere punitivo dello Stato» (cito dal resoconto sommario del convegno diffuso da Agorà e ripreso da MC-link).

In queste foto, alcuni dei partecipanti al convegno di Pesaro. Il giudice Gianfranco D'Aietti.

Leggiamo la Costituzione

E proprio dalla Costituzione è partito l'intervento di Vincenzo Zeno-Zencovich, avvocato e docente all'Unversità di Sassari, che è uno dei più noti studiosi italiani di informatica giuridica.

Alla base della normativa da emanare, ha detto Zeno-Zencovich, devono esserci gli articoli 2, 15, 21 e 41 della Costituzione, e alla luce di questi bisogna distinguere i diversi tipi di comunicazioni telematiche. «Dove l'attività telematica è comunicazione tra persone (due o più soggetti, quindi numero determinabile), essa è da considerarsi comunicazione non pubblica, ed è inserita quindi in un contesto che la qualifica come comunicazione interpersonale e riservata e, quindi, riconducibile all'art. 15 della Costituzione. Del resto l'articolo 15 tutela la libertà e la segretezza delle comunicazioni: la tutela è illimitata (mentre l'art. 21 incontra molti limiti) e non è previsto nemmeno il limite del buon costume, segno che il costituente ha voluto attribuire una libertà molto ampia». Su questo punto torneremo più avanti, a proposito delle opinioni del magistrato Carlo Sarzana di Sant'Ippolito.

Ancora dal convegno di Roma, va richiamata l'opinione di un altro magistrato, Giovanni Buttarelli, sul tema della professionalità degli operatori giudiziari. Buttarelli ha ricordato l'articolo 359 del Codice di procedura penale, «che obbliga il giudice ad avvalersi di esperti, ma forse occorrerebbe che il codice prevedesse espressamente periti informatici a disposizione, oltre che del magistrato, anche della polizia giudiziaria».

Lo spazio, come si dice, è tiranno, e non consente di dare conto diffusamente degli altri interventi, tutti interessanti. Va comunque citata la relazione di di Fabio Vitali, del CIRFID di Bologna, su un caso di pirateria telematica che ha coinvolto il centro dell'Università bolognese e quello della Statale di Milano, risolto attraverso un attento monitoraggio dell'attività del «cracker» e una serie di intercettazioni telefoniche. Dall'intervento di Vitali, e da un'animata discussione informale sorta alla fine del convegno, è emerso un problema molto grave: spesso gli operatori dei sistemi universitari, assorbiti da altre importanti attività, non possono dedicare la necessaria attenzione agli aspetti della sicurezza, come l'identificazione certa degli utenti che accedono alle reti dall'esterno degli atenei.

Occorre fare chiarezza

Una singolare coincidenza ha fatto sì che il convegno «Criminalità informatica e protezione del software: la tutela offerta dalla nuova normativa» si sia svolto a Pesaro, la città dalla quale è partita l'operazione Fidobust. Organizzato dall'IPACRI e dalla locale Cassa di Risparmio, l'incontro pesarese ha fornito nuovi elementi di discussione. Naturalmente l'intervento più atteso era quello di Gaetano Savoldelli Pedrocchi, il Procuratore della Repubblica che, autorizzando l'azione della Guardia di Finanza, ha suscitato il pandemonio seguito ai sequestri di maggio. Savoldelli Pedrocchi, in due appassionati interventi, ha confermato le cose che aveva detto nella conferenza stampa di pochi giorni prima, che abbiamo ampiamente riportato nel numero di luglio-agosto. In sostanza il Procuratore afferma che nelle attività illegali dei BBS il problema della pirateria del software è meno grave del-

le intrusioni illecite nei sistemi telematici e nella sfera della riservatezza degli individui, oltre che delle altre azioni criminose che possono passare attraverso i sistemi telematici. È la tecnologia, ha concluso Savoldelli Pedrocchi, che deve darci gli strumenti per la difesa dalle attività illecite, il diritto può fare poco e comunque non può limitare la libertà di comunicazione allo scopo di reprimere i reati.

Di diverso avviso, sotto molti punti di vista, il «padre storico» della legge sui reati informatici, Carlo Sarzana di Sant'Ippolito. I due magistrati hanno polemizzato, scambiandosi con perfetto garbo stilettate brucianti e destando qualche stupore con posizioni a prima vista insospettabili: il grande inquisitore Savoldelli si è rivelato molto più possibilista e garantista di Sarzana, co-autore della 547, da tutti giudicata una legge molto equilibrata. Le opinioni di quest'ultimo meritano un'attenzione particolare: l'intervista è nelle prossime pagine.

I due convegni, e il dibattito che li ha preceduti e che continua, hanno messo in luce alcuni punti che devono assolutamente essere chiariti. Il più importante è la necessità di mettere a fuoco l'insieme dei problemi giuridici posti dallo sviluppo della telematica. Non possiamo parlare solo di BBS, sia perché esse rappresentano solo una parte dei traffici telematici che si intrecciano su tutto il globo (e per questo è necessario armonizzare le normative dei diversi Paesi), sia perché i BBS stessi comprendono attività di diversa natura giuridica. Ciascuna di queste attività deve essere regolata da disposizioni specifiche. Un sistema telematico può essere assimilabile a un sistema postale, oppure a una pubblicazione, oppure a un archivio di informazioni. Per il primo caso c'è un soggetto che fornisce un servizio di caselle elettroniche e non interviene sul loro contenuto; per il secondo è indiscutibile la necessità di un responsabile a norma delle leggi sulla stampa, con alcune modifiche in funzione delle minori possibilità di controllo sui contenuti; per il terzo occorre un responsabile delle informazioni e del loro uso. Solo per quest'ultimo settore sono in discussione, da anni, norme per la tutela dei dati individuali. Per il resto non esiste alcuna regolamentazione, non solo in Italia, ma anche negli altri Paesi industrializzati. L'allarme ripetutamente lanciato sulle possibilità di utilizzo dei sistemi telematici da parte della criminalità organizzata rende urgente l'emanazione di una legge che stabilisca precise regole di comportamento per i gestori e per gli utenti; ma queste regole non devono comprimere la libertà di espressione e il diritto alla riservatezza degli individui, se non nei limiti stabiliti dalla Costituzione. E per questo bisogna valutare con attenzione la diversa natura giuridica dei singoli servizi.

Il problema della responsabilità

Bisogna finalmente capire che non ha senso affermare in astratto che un BBS deve avere, o non avere, un direttore responsabile dei contenuti come un giornale. Se il BBS è una «bacheca elettronica», cioè se contiene informazioni accessibili a una generalità di utenti, esso è senza dubbio una «pubblicazione», e deve quindi avere un direttore responsabile, i cui obblighi dovranno essere precisati in funzione delle caratteristiche specifiche del mezzo. Ma se un sistema telematico non comprende «aree pubbliche», il direttore responsabile non serve. Le comunicazione da un individuo a un altro, o a più individui identificati, sono a tutti gli effetti «corrispondenza», e ad esse devono essere applicate le norme che regolano questa attività. Il primo caso rientra delle disposizioni dell'articolo 21 della Costituzione, come osserva correttamente Zeno-Zencovich, e quindi il bene primario da tutelare è la libertà di espressione; il secondo ricade sotto la previsione dell'articolo 15, che sancisce l'inviolabilità della sfera privata.

Ma se un sistema telematico comprende ambedue le attività? È chiaro che, con le leggi oggi in vigore, il direttore responsabile della bacheca elettronica non può avere alcuna responsabilità sui messaggi privati, anzi, se li legge commette il reato di violazione della corrispondenza. Al contrario, il gestore di un servizio di caselle personali deve tutelare la riservatezza dei messaggi depositati ed è vincolato al segreto sulle informazioni delle quali venga casualmente a conoscenza.

Ma a questo punto si pone il problema della difesa dalle attività criminali. Che succede se una casella viene utilizzata per la trasmissione di informazioni su traffici illeciti? Se il gestore non può leggerne il contenuto, evidentemente non può essere perseguito per i reati che possono essere commessi attraverso la sua struttura. Ma allora, come verificare che i sistemi di posta elettronica non siano utilizzati per scopi criminali, anche in considerazione del fatto che l'intercettazione delle trasmissioni di dati è sempre più spesso ai limiti dell'impossibile?

Attenzione, non stiamo parlando di semplici scambi o vendite di software copiato abusivamente, un reato modesto, con buona pace delle associazioni dei produttori.

Stiamo parlando di mafia, di traffici di droga o di armi, di terrorismo, insomma di attività criminali che destano un altissimo allarme sociale.

E il livello dell'allarme sociale può giustificare compressioni della libertà dei singoli o dell'intera collettività. Ma entro quali limiti? ▶

Carlo Sarzana di Sant'Ippolito, presidente aggiunto GIP al tribunale di Roma.

Ultim'ora

USA, marcia indietro sul Clipper-chip

Clinton e Gore hanno fatto marcia indietro sul progetto Clipper, che prevedeva l'inserimento obbligatorio in ogni sistema informatico di un chip crittografico, che consentisse alle autorità l'intercettazione delle trasmissioni in codice. La reazione dell'opinione pubblica era stata negativa.

Sia per le difficoltà oggettive di intercettare flussi di dati tra modem ad alta velocità, con compressioni e correzioni d'errore, sia per i problemi che sarebbero derivati nell'esportazione di sistemi costruiti negli USA, l'amministrazione statunitense ha ora limitato l'applicazione del provvedimento ai centralini telefonici digitali.

Sarzana: tra privacy e sicurezza

Carlo Sarzana di Sant'Ippolito, oggi presidente aggiunto dell'ufficio del GIP presso il Tribunale penale di Roma, è uno dei magistrati italiani più attenti ai prolemi del diritto dell'informatica. I suoi interventi al convegno di Pesaro sono sembrati, su qualche punto, in contrasto con le opinioni più diffuse, espresse da molti partecipanti. Ma sono fondati su dati di fatto molto gravi, che dobbiamo tenere ben presenti quando parliamo di regolamentazione dei sistemi telematici.

* * *

***D**ottor Sarzana, le opinioni che lei ha espresso sui problemi della telematica vanno spesso controcorrente, e in qualche caso sembrano addirittura in contrasto con alcune disposizioni della legge sui crimini informatici, che lei stesso ha scritto o contribuito a scrivere...*

La mia relazione è stata svolta quasi a braccio, seguendo solo a volte una traccia scritta. Non so quali siano state le opinioni che, secondo lei, sarebbero addirittura in contrasto con la legge N. 547 del '93, legge che ho in realtà contribuito a redigere e della quale all'epoca ho seguito anche, in qualità di membro dell'ufficio legislativo del Ministero della Giustizia, l'iter parlamentare. Ho illustrato anzitutto come è nata l'idea di predisporre anche in Italia una legge contro la criminalità informatica, ed ho accennato al ruolo importante svolto al riguardo da due ministri della Giustizia, Vassalli prima e Conso poi. La mia esperienza, anche internazionale, nel campo del rapporto tra criminalità e tecnologia, mi ha consentito di fornire una consistente base di conoscenza alla Commissione ministeriale che ha predisposto la prima stesura del disegno di legge, destinato a divenire, con qualche modifica, la 547. La funzione propulsiva, per così dire, da me svolta rispetto al disegno di legge in questione, conosciuta all'esterno, mi è valsa poi la qualifica di «padre storico» della legge, e anche qualche inconsistente attacco da parte di alcuni «cyberpunk» italiani, attacco incautamente raccolto da un noto quotidiano politico. Ciò premesso, nella mia relazione ho cercato di chiarire qualche equivoco, nato soprattutto a seguito di frettolose letture delle norme effettuate da parte di pseudo/giuristi, ed anche di fornire la mia personale interpretazione in ordine all'attuazione pratica di alcune disposizioni della legge 547. Credo di aver contribuito ad una prima interpretazione autentica della legge, senza per altro avere la presunzione di affermare che non esistano oscurità o lacune nella regolamentazione.

***C'**è qualcosa di più di una lacuna, c'è una legge ancora da scrivere, che riguarda i sistemi telematici, e non solo i BBS più o meno cyberpunk. Ci sono le messaggerie pubbliche, le caselle elettroniche personali, gli aspetti giornalistici. Insomma, c'è la posta, c'è il broadcasting, c'è quello che gli americani chiamano «narrowcasting». Quali regole devono essere dettate, secondo lei?*

Carlo Sarzana di Sant'Ippolito.

Quando si parla di BBS occorre anzitutto chiarire la differenza tra «messaggeria» e «corriere elettronico». Per «messaggeria», che i francesi chiamano «tableau d'affichage», si deve intendere la cosiddetta «lavagna elettronica», sulla quale qualsiasi utente, spesso coperto dall'anonimato, inserisce un suo messaggio o annunzio, rivolto alla generalità degli utenti della rete (o delle reti, nel caso di reti collegate). I veri e propri sistemi di posta elettronica, almeno in Italia, sono riservati allo Stato, che può darli anche in concessione ai privati. Le «caselle postali elettroniche» sono quelle gestite nell'ambito delle reti BBS; questo tipo di corrispondenza telematica deve, a mio avviso, considerarsi chiusa, nel senso di cui all'articolo 616 del Codice penale, perché la zona in cui è il contenuto il messaggio può essere normalmente raggiunta soltanto dal titolare della casella. È da tener presente, peraltro, che il codice postale contiene la definizione di ciò che deve intendersi per «corrispodenza» ai fini delle leggi postali. Per quanto riguarda la regolamentazione dei BBS, per quello che io so, nessun paese al mondo ha provveduto a dettarla, probabilmente perché questo tipo di comunicazione interpersonale è visto dai legislatori con diffidenza, a causa dei possibili illeciti che possono commettersi mediante il suo uso. Passando ora a trattare il problema della responsabilità giuridica del sysop, credo sia banale premettere che questi sa bene, in genere, che tipo di traffico si svolge nell'ambito della sua rete. Può quindi cautelarsi stabilendo precise condizioni per l'accesso al sistema da parte degli aspiranti utenti e per il corretto utilizzo del sistema stesso. Tra queste condizioni vi dovrebbe essere anche quella relativa alla possibile esclusione dal servizio nel caso di violazione degli obblighi di correttezza da parte dell'utente. Il sysop, al fine di esercitare il suo legittimo controllo sulla regolarità del servizio, deve riservarsi esplicitamente il diritto di penetrare, nei casi sospetti, nell'interno delle singole caselle e controllare quindi il contenuto dei messaggi esistenti, avvalendosi della disposizione di cui all'articolo 51 del Codice penale (*per il quale l'esercizio di un diritto esclude la punibilità, ndr*). Devo precisare però che per il sysop non sembra sussistere l'obbligo del segreto, per cui non potrebbe applicarsi, nel caso nel caso di rivelazione del contenuto della corrispondenza telematica, la norma di cui all'articolo 620 del Codice penale (*rivelazione del contenuto di corrispondenza commessa da persona addetta al servizio, ndr*), in quanto il sysop non può considerarsi, allo stato, un «addetto al servizio delle poste, dei telegrafi e dei telefoni». E d'altro canto, nel campo del diritto penale è vietato il ricorso all'analogia. Va tenuto presente in argomento, e qui lo rilevo *per incidens*, che il legislatore non ha ritenuto di dover punire il prendere semplicemente cognizione di una comunicazione o conversazione informatica o telematica (diversa dalla «corrispondenza»). Infatti l'articolo 617 quater, a differenza dell'articolo 617, non contempla tale ipotesi, e cioè «la cognizione», ma soltanto «l'intercettazione, l'impedimento e l'interruzione illecita di comunicazioni informatiche o telematiche».

***S**e ho capito bene, lei dice: stabiliamo che il contenuto della casella elettronica non è assimilato alla corrispondenza, ma a «oggetti postali» come le stampe, che possono essere aperte dal gestore del servizio. Ma, se guardiamo i fatti, la natura dei messaggi di posta elettronica è personale, è «corrispondenza». E dunque si pone forse un problema di legittimità di una norma che stabilisca il diritto del sysop di leggerla. C'è di mezzo l'articolo 15 della Costituzione. E per il sysop c'è l'impossibilità materiale di controllare tutto. Inoltre bisognerebbe anche vietare la cifratura dei messaggi.*

No, per questo basterebbe obbligare l'utente a comunicare al sysop la chiave crittografica e ogni sua variazione. I controlli possono essere fatti a campione. E poi un sysop che si rispetti conosce bene i suoi polli. C'è un pericolo molto grave per i BBS, che non è stato avvertito: la possibilità che il Ministero dell'Interno, e non sto parlando a caso, possa preparare una disposizione di legge che consenta l'intercettazione su tutto il territorio nazionale di non importa quale BBS, anche al di fuori di un

provvedimento specifico e mirato della magistratura, cioè richiedendo un provvedimento generico al giudice.

Questa è dura da digerire!

È dura, ma se continuano così... C'è già qualche precedente da questo punto di vista, per quanto riguarda i telefoni cellulari, quindi non è azzardato immaginare una cosa di questo tipo. È lo stesso discorso della direttiva Clinton: l'FBI sostiene la necessità di inserire in tutti i sistemi un chip che consenta le intercettazioni, proprio perché con il mutamento delle chiavi crittografiche non riesce più a intercettare il contenuto delle comunicazioni. Il discorso diventa delicatissimo per il bilanciamento tra il rispetto della «privacy» e il diritto dello Stato di proteggere l'ordine pubblico e di proteggersi dalla criminalità organizzata. Bisogna fare un discorso chiaro, pubblico, trasparente, e poi si potrà arrivare a una decisione. È il discorso fra iniziati o dietro le quinte che io non approvo, perché ci sono in ballo i due grandi valori: il diritto alla privacy e il diritto dello Stato di proteggere i cittadini. Bisognerà vedere se è possibile un bilanciamento o, in caso di impossibilità, quale dei due valori debba prevalere. Ma bisogna che vi sia un dibattito pubblico su questo.

***È** quello che noi, come rivista, stiamo cercando di fare. Noi sosteniamo che l'accesso anonimo in scrittura a qualsiasi sistema telematico debba essere vietato, senza eccezioni, e che il gestore debba essere obbligato a identificare l'abbonato. Questo potrebbe risolvere molti problemi: solo con l'accesso anonimo si possono scambiare impunemente password rubate, programmi copiati illegalmente e cose del genere. Nel momento in cui chiunque acceda in scrittura a un sistema telematico sia preventivamente identificato, la possibilità di usare la posta elettronica per commettere reati si riduce notevolmente.*

E, naturalmente, con un log che registri tutti gli accessi... Io farei una cosa molto semplice. Se fossi un sysop, tenterei di mutuare per il sistema di posta elettronica le disposizioni in materia di casella postale. Perché, se quelle disposizioni sono valide per lo Stato, possono e devono essere valide per i privati. Per ottenere una casella dal servizio postale, occorre una richiesta motivata, c'è l'identificazione del richiedente.

Ma il servizio postale non va ad aprire le buste che vengono messe nelle caselle!

Questo no, a meno che non ci siano particolari motivi per ritenere che si debbano fare eccezioni alla regola generale del segreto epistolare. Però, se lei non accetta il mio presupposto, non ne usciremo mai. Non accettare il presupposto, e cioè una forma di autoregolamentazione che renda il sysop responsabile, farà intervenire sistematicamente l'autorità giudiziaria. C'è il forte rischio della messa sotto sorveglianza delle BBS, con l'autorizzazione dell'autorità giudiziaria, e la forte tentazione di avere la possibilità di accedere a qualsiasi rete, non importa in quale luogo del territorio nazionale, mediante un sistema permanente di controllo. Il sysop, se vuole diventare una figura riconosciuta, deve assumersi le sue responsabilità.

***C**erto, ma forse l'autoregolamentazione non basta. Le responsabilità del gestore devono essere stabilite dalla legge, e potrebbero, a nostro avviso, essere inserite nella legge sulla protezione dei dati personali, che prima o poi vedrà la luce.*

Ho molti dubbi che possano essere inserite in quel disegno di legge, perché l'oggetto è totalmente diverso. Delle disposizioni speciali per la corrispondenza telematica potrebbero rappresentare una «coda», per così dire, del codice postale.

***U**n altro argomento di discussione è la configurabilità di un sistema telematico come una pubblicazione giornalistica, con la nomina di un direttore responsabile. Lei è d'accordo su questo punto?*

Sicuramente. Quando c'è un «tableau d'affichage», c'è la possibilità di diffamazione.

***P**erò nella messaggeria pubblica elettronica, il direttore non ha la possibilità di controllare i contenuti prima che vengano messi in linea, come accade invece in un giornale stampato. E che facciamo, mettiamo le manette al gestore ogni volta che qualcuno scrive un messaggio offensivo?*

No, bisognerebbe creare una forma di responsabilità non oggettiva, diversa da quella stabilita per la stampa. C'è una difficoltà di intervento tempestivo da parte del sysop, e bisogna quindi configurare una responsabilità specifica per dolo o colpa, ma non una responsabilità oggettiva, perché per la carta stampata il controllo è semplice, per i sistemi elettronici non lo è. Bisogna considerare che sono accadute cose molto spiacevoli: a questo riguardo, in Francia mi pare, ci sono stati casi di persone che hanno perso addirittura il posto di lavoro per notizie immesse nelle messaggerie pubbliche. Sarebbe comunque già un passo avanti l'eliminazione dei messaggi anonimi.

***C**erchiamo di riassumere. Al primo punto mettiamo la proibizione totale dell'anonimato, poi la facoltà, o l'obbligo, per il gestore di andare a leggere nelle caselle personali...*

Il controllo deve essere un diritto del sysop. Deve esistere per chi chiede la «casella» l'obbligo di sottostare ad eventuali controlli, così come l'obbligo per il gestore di conservare il segreto. C'è già la norma sulla rivelazione dei contenuti della corrispondenza, ma sarebbe utile richiamarla espressamente per il sysop che effettua questi controlli.

***M**a il gestore non può controllare tutti i messaggi, e quindi potrebbe sfuggirgli qualcosa di illegale. In questo caso quale sarebbe la sua responsabilità?*

Non dovrebbe essere responsabile in caso di negligenza, a meno che non venga inserita nella normativa anche una responsabilità per colpa. È sempre un problema di fatto. Esistono motivi per cui con la normale diligenza era possibile accorgersi di un traffico illegale? Quando abbiamo previsto il diritto del sysop di controllare la casella postale, e l'obbligo del titolare della casella di sopportare il controllo, abbiamo fatto metà del lavoro. A questo punto ci si potrebbe chiedere: il sysop che sa che si sta svolgendo un'attività illegale, spesso anche grave, che cosa deve fare? Potrebbe prevedersi l'obbligo di denuncia solo per alcuni gravi reati. Nel caso di commissione di reati scatterebbe però per il sysop una responsabilità in ordine all'interruzione del servizio. Bisognerà vedere come configurare l'eventuale omissione, come sanzionarla. Esiste la necessità di una specie di rapporto all'autorità giudiziaria, per reati di grave entità. Per esempio se la casella postale serve come transito di informazioni per un traffico di droga.

***A**ltrimenti diventa favoreggiamento.*

Certo. Ma stracciarsi le vesti, invocare la libertà di informazione, di circolazione delle idee, per far passare liberamente informazioni illegali, è paradossale, lo trovo addirittura puerile. Ci sono regole del vivere sociale e regole del diritto penale che devono essere osservate. Chi non vuole osservarle si pone al di là del diritto.

***A** partire dalla 547...*

Senza la 547 l'Italia sarebbe diventata il paradiso della criminalità informatica, e chi è contrario a questa normativa vuole semplicemente il caos, vuole che nel nostro Paese sia possibile commettere qualsiasi crimine informatico, senza neppure la possibilità di azionare gli strumenti di cooperazione internazionale, che richiedono una certa reciprocità per quanto riguarda le infrazioni. D'altro canto, dobbiamo emanare anche norme che impongano in qualche modo un training per gli investigatori. Da sondaggi che sono stati fatti in tutto il mondo è emerso che uno dei motivi principali per cui le vittime di reati informatici spesso non li denunciano, è la sfiducia nella capacità operativa e nell'esperienza della polizia e della magistratura.
E se la gente legge storie come quella dei sigilli messi a una camera da letto, è difficile che possa nutrire fiducia nell'opera degli investigatori. MC ▶

Claudio Gerino, del quotidiano «la Repubblica»: è difficile informare su argomenti che il pubblico conosce poco.

◀ *Gaetano Savoldelli Pedrocchi, procuratore della Repubblica di Pesaro.*

Lettere e cartoline

Le affermazioni di Sarzana, oltre a richiedere qualche spiegazione per i non addetti ai lavori, impongono una riflessione particolarmente attenta, in considerazione dell'autorevolezza della fonte dalla quale sono espresse.

· Quando il magistrato parla della differenza tra il disposto dell'articolo 617 e quello del 617-quater del Codice Penale, rivela un particolare della legge 547/93 sfuggito a molti. L'art. 617 recita: *(Cognizione, interruzione o impedimento di comunicazioni o conversazioni telegrafiche o telefoniche). Chiunque, fraudolentemente, prende cognizione di una comunicazione o di una conversazione, telefoniche o telegrafiche, tra altre persone o comunque a lui non dirette, ovvero le interrompe o le impedisce, è punito con la reclusione da sei mesi a quattro anni.* Invece l'articolo 417-quater dice: *(Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche). Chiunque fraudolentemente intercetta comunicazioni relative ad un sistema informatico o telematico, o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni.* La differenza è sostanziale: mentre l'articolo 617 punisce anche la «cognizione» dei contenuti delle comunicazioni telefoniche o telegrafiche, oltre all'interruzione e all'impedimento, il 617-quater non considera la semplice presa di conoscenza, sia pure illecita. Cioè, se qualcuno va a mettere il naso in una qualsiasi comunicazione telematica al solo scopo di conoscerne il contenuto, non commette reato. È vero che l'intercettazione (cioè la cattura di informazioni nel momento in cui passano da un sistema all'altro) è comunque punita, ma chi vada a leggere il contenuto di una casella personale non «intercetta», bensì «prende cognizione». Quindi per l'articolo 617-quater, il sysop che legge i messaggi personali depositati nella sua BBS non commette alcun reato?

No, perché le comunicazioni previste dal 617-quater sono evidentemente diverse dalla «corrispondenza», tutelata dall'art. 616, innovato con la nuova formulazione del quarto comma dell'art. 616, introdotta dalla 547. Dice il 616: *(Violazione, sottrazione e soppressione di corrispondenza). Chiunque prende cognizione del contenuto di una corrispondenza chiusa, a lui non diretta, ovvero sottrae o distrae, al fine di prendere o di farne da altri prendere cognizione, una corrispondenza chiusa o aperta, a lui non diretta, ovvero, in tutto o in parte, la distrugge o la sopprime, è punito... con la reclusione fino a tre anni.* Il nuovo testo del quarto comma precisa: *Agli effetti delle disposizioni di questa sezione, per «corrispondenza» si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza.* Dunque il sysop che legga il contenuto di una casella personale non viene punito sulla base del 617-quater, ma va in galera per aver violato il 616. Osserva infatti Sarzana che «questo tipo di corrispondenza telematica deve considerarsi chiusa, nel senso di cui all'articolo 616 del Codice penale».

E un'attenta lettura del 616 fa luce sul problema: è punita la semplice presa di cognizione della corrispondenza «chiusa», non di quella «aperta». È addirittura banale, chiunque può leggere una cartolina! E allora basterà emettere una norma piccola piccola, che stabilisca che il contenuto di una casella elettronica non è una «lettera» ma una «cartolina», per autorizzare il gestore del sistema a prenderne conoscenza (ma resterebbe la proibizione di diffonderne il contenuto). Insomma, il 617-quater è una bomba a orologeria, che potrebbe scoppiare al momento della tanto auspicata regolamentazione dei sistemi telematici.

L'avvento del Grande Fratello

Il «padre storico della 547» si rende perfettamente conto del potenziale dirompente di questa norma e delle reazioni che può suscitare. Conferire al sysop il diritto di frugare nella corrispondenza dei suoi abbonati costituirebbe un'imitazione del diritto alla riservatezza e diminuirebbe il valore sociale della posta elettronica. Ma Sarzana giustifica la sua posizione con un avvertimento: attenzione, se non facciamo così, se non diamo al gestore del sistema una responsabilità pubblica per il controllo dei contenuti, altri potrebbero mettersi a controllare in modo ancora più invadente e limitativo del diritto alla riservatezza di tutti i cittadini.

Insomma, per combattere la criminalità potrebbe essere varata una norma che allarghi i limiti entro i quali la magistratura può autorizzare le intercettazioni. Oggi le forze dell'ordine possono essere autorizzate a compiere intercettazioni solo per reati di particolare gravità e con una serie di vincoli posti a tutela della privacy degli individui; domani, sull'onda di fatti criminosi particolarmente gravi, si potrebbe arrivare ad intercettare tutto e tutti. Il Grande Fratello è dietro la porta? Si può ipotizzare un così brusco passaggio da una democrazia, sia pure imperfetta, a uno «Stato di polizia»? «Non sto parlando a caso», dice il magistrato, «c'è già qualche precedente».

Prospettive molto preoccupanti. Anche perché c'è il rischio che le ipotizzate restrizioni della privacy non servano a combattere la criminalità: nel momento in cui la posta elettronica si rivelasse insicura per far passare impunemente informazioni illegali, i delinquenti sceglierebbero altri mezzi di comunicazione. E ai cittadini onesti resterebbe solo la limitazione della libertà di trasmettere riservatamente il proprio pensiero.

Dobbiamo cercare altre strade.

MC

TRAVELMATE serie M

Una nuova generazione di notebook con slot PCMCIA, dispositivo di puntamento integrato, funzioni audio e gestione immagini in movimento.

TUTTO QUELLO CHE AVRESTE VOLUTO DA UN NOTEBOOK
POTENZA, SUONO, ANIMAZIONE

I nuovi TravelMate 4000 M sono in grado di elaborare, registrare e riprodurre suoni con la stessa qualità del Vostro HI-FI, grazie al sistema audio a 16 bit SoundBlaster Pro compatibile, interfaccia MIDI, altoparlante e microfono incorporati.
Contemporaneamente possono riprodurre immagini in movimento su fantastici display a colori, sfruttando la combinazione di una sofisticata tecnologia implementata da Texas Instruments e Intel Indeo™ Video.
La sorprendente potenza elaborativa (fino a 75 MHz) e la notevole autonomia (da 3 a 5 ore) sono senza compromessi.
Espandibilità e connessioni sono di serie: slot per schede PCMCIA type III e interfaccia FAST SCSI II. Tutto in soli 2,9 Kg di peso batterie incluse.
Ma non è finita! Aggiungendo CD-ROM Docking System Portatile (2 Kg di peso batterie incluse) avrete a disposizione un sistema multimediale completo, con CD-ROM a doppia velocità, altoparlanti stereo, cuffie e microfono esterno.

TravelMate 4000M/75
iDX4/75 MHz
HD 340 MB
Display Colore TFT

TravelMate 4000M/50
i486SX2/50 MHz
HD 340 / 200 MB
Display Colore TFT / DS

Portable Docking System
CD-ROM doppia velocità
Altoparlanti stereo,
cuffia e microfono

Per saperne di più, rivolgetevi ai Rivenditori Qualificati Texas Instruments o contattateci
Tel. 039-68421
Fax 039-652206

MICROSOFT WINDOWS

SoundBlaster Pro è un marchio registrato Creative Technology, Indeo, iDX4/75, i486SX2/50 sono marchi di Intel Corporation.

EXTENDING YOUR REACH
WITH INNOVATION

TEXAS INSTRUMENTS