

È urgente colmare il vuoto legislativo  
**«De iure condendo»**  
**(sulle leggi da fare)**

*La vicenda «Fidobust» ha messo in luce la mancanza di norme certe sulla telematica e sulle banche dati. Governo e Parlamento devono muoversi in fretta, il futuro è oggi*

*di Manlio Cammarata*



Il titolo di questo pezzo è un'espressione latina cara ai giuristi, e significa letteralmente «sul diritto da fondare». L'ho scelta perché queste note sono state redatte con la collaborazione di alcuni giuristi e sono rivolte anche al potere legislativo: ci sono leggi che devono essere fatte, o rifatte, con la massima urgenza.

Naturalmente il punto di partenza è «Fidobust», l'operazione della Guardia di Finanza ordinata dalla Procura di Pesaro, che ha portato alla chiusura di molti BBS in tutta Italia (*bust* si può tradurre come «pugno» o «bastonata»). L'azione ha ridotto in misura sensibile soprattutto l'attività della rete Fidonet, colpendo anche un nodo di Peacelink.

Nello stesso periodo, con indagini partite da Milano e da Torino, sono state identificate in tutta Italia diverse strutture dedite al traffico illegale di software. Pure coincidenze temporali? In parte sì, senza dubbio, perché da più di un anno la magistratura e le forze dell'ordine hanno iniziato a colpire la pirateria informatica, dopo l'entrata in vigore del DL 518/92 sulla protezione dei diritti degli autori del software. Tuttavia la vicenda di Fidonet e Peacelink ha destato molte perplessità tra gli addetti ai lavori, soprattutto perché ha colpito, insieme a presunti «pirati», alcune attività perfettamente legali. Nel caso di Peacelink, addirittura di grande rilievo umanitario (è impegnata, fra l'altro, negli aiuti ai

Paesi dell'ex-Jugoslavia e coordina un centro di soccorso aereo).

Per chiarire meglio il discorso, riassumo brevemente i fatti noti fino al 20 giugno. Tutto incomincia in febbraio con una comunicazione del Comando Generale della Guardia di Finanza al Nucleo di Ancona: si segnala l'esistenza, a Pesaro, di una struttura clandestina dedita alla pirateria del software su vasta scala. Il Procuratore della Repubblica autorizza le indagini, che comprendono anche intercettazioni sulle linee telefoniche, e l'11 maggio scattano perquisizioni e sequestri in tutta Italia. È la più vasta operazione mai compiuta nel mondo contro la pirateria informatica: 122 perquisizioni (in 33 casi non si trova nulla di illeciti

to), sequestrati 110.992 dischetti, 245 CD-ROM, 298 streamer, 159 personal computer e 83 modem. L'organizzazione di Pesaro è un «point» della rete Fidonet, e di conseguenza molte BBS di questa rete vengono ridotte al silenzio (sembra che siano una trentina), mentre altre preferiscono chiudere di propria iniziativa, nel timore di essere coinvolte. Con il sequestro delle attrezzature viene ridotto al silenzio anche un nodo di Peacelink.

### C'entra la politica?

L'eco dell'operazione è grandissima, e non solo in Italia, anche perché sono stati colpiti alcuni soggetti di una grande comunità che fa della comunicazione la propria ragione di esistere. Dell'*Italian BBS Crackdown* si occupano non solo le reti telematiche, ma persino la stampa estera. I BBS si riempiono di commenti, si cercano affannosamente informazioni precise sull'accaduto. Due aspetti colpiscono in modo particolare: il primo è la sostanziale interruzione di una parte della rete Fidonet, sia per i sequestri operati dalla polizia giudiziaria, sia per l'iniziativa spontanea di alcuni operatori; il secondo sono le modalità con le quali sono avvenuti i controlli, per lo più di notte, all'interno di abitazioni private, con il sequestro anche di materiali innocui, come le prese elettriche o i tappetini dei mouse, e in un caso apponendo addirittura i sigilli a una camera da letto («ma li ho fatti togliere subito», ha detto il magistrato di Pesaro, Gaetano Savoldelli Pedrocchi, in una conferenza stampa tenuta il 17 giugno).

Nelle settimane successive il «Tribunale del riesame» affronta ventidue ricorsi presentati dai legali degli indagati e ordina il dissequestro dei computer e l'affidamento dei dischi «in custodia giudiziaria» ai rispettivi proprietari. Il 3 giugno viene chiuso il nodo centrale di Peacelink a Taranto (con un'operazione non collegata a Fidobust e ordinata dalla locale Procura).

Le conseguenze di Fidobust sono tante e gravi, e vanno ben al di là dei danni eventualmente subiti da chi, innocente, sia caduto nella rete tesa dalla Guardia di Finanza di Ancona. L'operazione di polizia giudiziaria ha dimostrato in modo inconfutabile che la legislazione italiana in materia di informatica e telematica presenta carenze gravissime, che possono comprimere in diversi modi i diritti dei cittadini garantiti dalla Costituzione e produrre danni di notevole rilevanza sociale.

Basta scorrere le centinaia di messaggi pubblicati dopo l'11 maggio



In questa foto e in quella di apertura, due immagini scattate dalla Guardia di Finanza nel corso della prima perquisizione a Pesaro.



Un angolo del centro di duplicazione abusiva di Pesaro. Quando il crimine diventa industria, deve essere colpito con la massima severità.

nell'area «BBS Comments» di MC-link per capire quanti e quali problemi siano stati messi in luce da Fidobust e dall'azione contro Peacelink. Quest'ultimo caso ha sollevato anche voci preoccupanti su un possibile movente politico: il BBS, oltre alle azioni umanitarie, è anche collegato alla rivista «I Siciliani»,

una pubblicazione di grande impegno sociale, fondata da Giuseppe Fava, ucciso dalla mafia. L'impegno dei militanti per la pace ha rimesso in piedi e rafforzato la struttura telematica nel giro di ventiquattr'ore, ma sarebbe opportuno fare subito la massima chiarezza sui contorni di questa vicenda.

## Cinque problemi

Una prima valutazione dei fatti mette in luce una serie di aspetti che meritano la massima attenzione.

Primo. Se è giusto e opportuno procedere contro persone sulle quali esistono seri indizi che svolgano un'attività illegale, non è altrettanto giusto operare perquisizioni e sequestri a carico di altri soggetti, solo per il fatto che hanno avuto collegamenti telematici con i primi e svolgono lo stesso tipo di attività. L'equazione «telematica uguale pirateria» sarebbe stata l'inaccettabile causa dell'espansione delle indagini. La legge dice che la magistratura deve agire contro chi sia ragionevolmente sospettabile di aver commesso un reato, non contro chiunque svolga una certa attività, per accertare poi se, per caso, è innocente.

Secondo. Le perquisizioni sono state compiute, in molti casi, da personale non preparato sulla materia specifica, che ha proceduto sequestrando anche oggetti non direttamente connessi con i reati ipotizzati: interi computer, o addirittura le prese di corrente e i mouse. Anche questo è molto grave, perché così sono state interrotte attività perfettamente lecite: un PC serve a lavorare, a giocare, a scrivere una tesi di laurea... Vale la pena di ricordare che l'art. 159 della legge sul diritto d'autore (la 633/41, innovata dal DL 518/92 con le norme sul software) prescrive: *La rimozione o la distruzione... non può avere per oggetto che gli esemplari o copie illecitamente riprodotte o diffuse, nonché gli apparecchi impiegati per la riproduzione o diffusione, che, per loro natura, non possono essere adoperati per una diversa riproduzione o diffusione* (ne parliamo più avanti, nell'intervista con il giudice D'Aiotti). È come se, ordinando il sequestro delle copie di un giornale in seguito a una querela per diffamazione, il magistrato mettesse i sigilli anche alla redazione e alla tipografia, chiudendo di fatto la pubblicazione. E questo si è verificato con il sequestro delle apparecchiature di Peacelink, agenzia di notizie e coordinamento di un centro di soccorso aereo. Si può fermare il sistema informativo di un ospedale o di un centro per i trapianti d'organo solo perché c'è, o si sospetta che ci sia, software illegale in qualche computer?

Terzo. Non c'è dubbio che una certa percentuale di malandrini si annidi anche tra chi si serve delle reti telematiche, come abbonato o come gestore, e che anche in una struttura che si è data regole ferree di correttezza possano nascondersi aree illegali. Ma a questo punto bisogna stabilire chi sia responsa-



Telefoni e computer: la criminalità corre sui fili. Ed è una rincorsa continua tra pirati e specialisti della sicurezza.

bile di eventuali reati commessi attraverso queste strutture, quali siano i suoi compiti, quali precauzioni debba prendere per evitare di essere incriminato per reati commessi da altri.

Quarto. Si è detto e si dice che l'operazione Fidobust sia stata in qualche modo pilotata «politicamente» da qualcuno che avrebbe interesse a colpire la telematica amatoriale. Non esiste nessun indizio di un collegamento di questo tipo, ma non c'è dubbio che notizie come queste contribuiscono a diffondere nella gente una visione sbagliata della telematica, come se ogni possessore di modem fosse un hacker (e qui la stampa di informazione ha gravi responsabilità). Quindi fatti come questi possono oggettivamente favorire la politica di qualche grande organizzazione che si appresti a vendere una telematica «a denominazione d'origine controllata», schiacciando quella che nasce per iniziativa di gruppi di appassionati o di strutture commerciali non legate a potenti gruppi multinazionali.

Da questa considerazione nasce il quinto (ma forse non ultimo) problema: è necessaria anche una regolamentazione dell'accesso e dell'uso delle reti di telecomunicazioni, per evitare che si verificino situazioni come quella prodotta dalla troppo lunga assenza di leggi sull'occupazione delle frequenze per le trasmissioni televisive.

## La legge che manca

Dunque i nodi da sciogliere sono molti, e non riguardano solo la telematica amatoriale, che rappresenta una piccolissima parte del crescente traffico di informazioni digitalizzate. Nei giorni suc-

cessivi a Fidobust si è spontaneamente creato un dibattito tra gli appassionati di telematica, con lo scopo di elaborare una proposta di legge per la regolamentazione dei «bollettini» amatoriali. Decine di messaggi su questo argomento vengono depositati ogni giorno su MC-link. È un dibattito molto interessante, che mette in luce una certa maturità del settore, con una precisa consapevolezza dei meriti, dei limiti e dei rischi di questa attività. Tuttavia a tanto entusiasmo a volte non corrisponde un'informazione completa su tutti gli aspetti giuridici del problema. È quindi opportuno mettere a fuoco alcuni punti fondamentali.

Qual è in Italia la situazione legislativa per questo settore? Le leggi che in qualche modo regolano aspetti legati alle nuove tecnologie non mancano: l'Annuario di Diritto delle Tecnologie dell'Informazione, diretto da Donato Limone, consta di due tomi per un totale di quasi millecinquecento pagine (se ne parla nel riquadro). Ma si tratta per lo più di norme per l'impiego dell'informatica nelle pubbliche amministrazioni centrali e locali, o volte a regolare aspetti specifici in particolari settori. Per quello che ci interessa in questa sede, c'è l'abbondante produzione dell'Unione Europea e ci sono due leggi italiane, delle quali si è spesso parlato su queste pagine: il Decreto Legislativo N. 518 del 29 dicembre '92, sul diritto d'autore, e la legge 547 del 23 dicembre '93 sui crimini informatici (quest'ultima è stata emanata dopo la pubblicazione dell'Annuario). Ma questi due provvedimenti non esauriscono il quadro legislativo che dovrebbe regolare l'informatica e la telematica: mancano ancora le disposi-

zioni sulle banche dati e sull'archiviazione e la diffusione dei dati personali (la famosa «legge Mirabelli»), che da anni navigano inutilmente tra i due rami del Parlamento e il Ministero di Grazia e Giustizia. E proprio questa legge, opportunamente aggiornata al nuovo panorama delle «autostrade dell'informazione» dovrebbe risolvere molti dei problemi sollevati dall'operazione Fidobust.

Il DL 518/92 che, come ormai tutti sanno, modifica la legge 633/41 sul diritto d'autore, è stato emanato per adeguare la legislazione italiana alle prescrizioni comunitarie europee. Queste, è altrettanto noto, sono state dettate in buona parte sotto la pressione delle grandi case produttrici di software, e quindi rispecchiano impostazioni che non tengono nel dovuto conto anche le esigenze degli utilizzatori. Non a caso il primo commento apparso su questa rivista dopo l'emanazione del decreto si intitolava «Il software è protetto. E l'utente?» (MCmicrocomputer N. 129). A parte alcune incongruenze che potrebbero addirittura viziare di incostituzionalità il decreto stesso, come abbiamo visto sul N. 135, molte disposizioni appaiono vessatorie, mentre alcuni punti importanti non sono regolamentati. In particolare, manca qualsiasi indicazione per lo «shareware», programmi la cui duplicazione e libera diffusione è addirittura incoraggiata dagli autori, che chiedono solo una piccola quota di registrazione a chi decida di usare regolarmente il software. In alcuni casi la licenza che accompagna il programma limita a un determinato periodo di tempo il diritto di usarlo senza pagare la registrazione, in altri no. *Quid iuris*, quali norme regolano la detenzione di shareware per il quale non sono stati pagati i diritti? Certamente non quelle del DL 518 (nonostante l'opinione contraria della BSA, l'associazione dei produttori), che non prevede alcuna forma di libera circolazione di programmi. Oltre allo shareware esistono i programmi di pubblico dominio, mentre i diritti di utilizzo del «freeware» sono di solito elencati nella licenza che lo accompagna: tutto questo deve essere comunque regolamentato. Appare quanto meno eccessivo che la detenzione di shareware non registrato possa comportare azioni penali, con relativi sequestri. E sarebbe necessaria qualche forma di deroga per chi detiene copie di programmi solo a scopo di documentazione o di studio e, naturalmente, possa dimostrarlo. Insomma, si dovrebbe trovare una specie di definizione di «modica quantità», di una «dose giornaliera» che comprenda anche il caso di software obsoleto o non più in circolazione, perché è chiaro che nes-

sun danno può derivare all'autore da qualche copia abusiva di un programma da tempo fuori commercio.

### Le norme per i BBS

Ancora più grave appare la mancanza di una legge che regolamenti l'attività delle strutture telematiche, e questo giustifica le discussioni sorte in questo periodo tra gli appassionati e le proposte che vengono avanzate. Ma il problema non è semplice come sembra. In particolare devono essere valutati con molta prudenza i progetti che prevedono una registrazione dei BBS presso le Questure o altre autorità. Se fosse stata

approvata la legge sulle banche dati, molti «bollettini» amatoriali ricadrebbero in questa fattispecie e sarebbero soggetti alla notifica al «Garante dei dati», con tutta una serie di pesanti obblighi di gestione. Ma, a mio avviso, la necessità di un'autorizzazione di polizia, quasi implicita nel concetto di «notifica», è inaccettabile. Gestire un BBS amatoriale è un'attività in sé non pericolosa, del tutto pacifica, educativa, in qualche caso socialmente utile. Chiedere una registrazione alla Questura (o al Commissariato, che è la stessa cosa), è come obbligare a registrarsi un collezionista di francobolli o di vasi cinesi. Anche la proposta di un patentino, subor-

#### Art. 3.

1. Dopo l'articolo 491 del codice penale è inserito il seguente:

«Art. 491-bis. - (Documenti informatici). - Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli».

#### Art. 4.

1. Dopo l'articolo 615-bis del codice penale sono inseriti i seguenti:

«Art. 615-ter. - (Accesso abusivo ad un sistema informatico o telematico). - Chiunque abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha il diritto di escluderlo, è punito con la reclusione fino a tre anni.

La pena è della reclusione da uno a cinque anni:

1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

*Per la legge 547 non ci sono più differenze sostanziali tra documenti cartacei e documenti informatici. Inserirsi in un sistema informativo altrui è reato anche se non si danneggia nulla.*

#### Art. 5.

1. Nell'articolo 616 del codice penale, il quarto comma è sostituito dal seguente:

«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».

#### Art. 6.

1. Dopo l'articolo 617-ter del codice penale sono inseriti i seguenti:

«Art. 617-quater. - (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.

Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma.

I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa.

Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

1) in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

2) da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

3) da chi esercita anche abusivamente la professione di investigatore privato.

dinato al superamento di un esame, non sta in piedi, perché i rischi di disturbare altri utenti non sono gli stessi delle trasmissioni radio. L'unica possibilità di provocare inconvenienti nelle reti di telecomunicazioni deriva dall'uso particolarmente maldestro di vecchi modem non omologati. Un «sysop» incompetente può danneggiare solo se stesso, mandando in crash il suo sistema, e so-

no fatti suoi. Naturalmente questo vale per le attività puramente amatoriali, senza alcun fine di lucro. Per le strutture commerciali il discorso è diverso, e occorre una regolamentazione che potrebbe essere inserita nella legge sulle banche dati.

Un altro problema riguarda invece le informazioni contenute nella posta elettronica, che costituisce buona parte

dell'attività dei BBS amatoriali. E qui bisogna distinguere. Per quanto riguarda le messaggerie basate su caselle personali, esse devono essere considerate come normale corrispondenza cartacea: la legge 547/93 è chiarissima su questo punto, quando afferma che per «corrispondenza» si intende quella epistolare, telegrafica, telefonica, informatica o telematica, ovvero effettuata con ogni altra forma di comunicazione a distanza (art. 616 CP, comma 4). Dunque è segreta, e il gestore che andasse a leggerla commetterebbe un reato, esattamente come un postino che aprisse le lettere affidategli per il recapito. Nel caso di comunicazioni pubbliche (chat o messaggi che possono essere letti da tutti gli abbonati) il discorso si fa più complesso, perché attraverso questo tipo di messaggeria si possono commettere reati come la diffamazione, si possono diffondere notizie riservate e così via. Sarebbe evidente, a prima vista, la responsabilità del gestore, che è o può essere assimilato al direttore responsabile di una pubblicazione stampata o radiotrasmissa. Ma qui c'è un problema: un sysop non ha materialmente la possibilità di controllare il contenuto dei messaggi prima che vengano diffusi; sarebbe necessario imporre il deposito preventivo delle comunicazioni in un'area riservata al responsabile, che le metterebbe in linea dopo averle lette. Ma questo sarebbe contrario alla natura stessa della maggior parte dei BBS. Bisogna invece stabilire, per legge o per regolamento del BBS stesso, che chi scrive è l'unico responsabile dei contenuti. Ma qui ci troviamo di fronte alla questione più importante: l'identificazione di chi scrive un messaggio. Il gestore dovrebbe infatti essere considerato responsabile di tutte le comunicazioni delle quali non sia identificato o identificabile il mittente. Per i messaggi privati il gestore dovrebbe indicare chiaramente qual è il loro livello di segretezza, in particolare se possono essere letti o no da chi ha un accesso privilegiato al sistema, e per i messaggi pubblici dovrebbe avere la facoltà di cancellare quelli che riteneva potenzialmente dannosi per il sistema.

### Contro gli hacker

L'obbligo assoluto e inderogabile di identificare chiunque acceda in scrittura ad un sistema telematico può non piacere ai fautori della totale libertà di modem. Ma non bisogna dimenticare che la libertà di ciascuno finisce sul punto in cui limita o mette in pericolo la libertà degli altri. E i crimini che possono essere commessi attraverso un modem sono troppi e troppo gravi per non richie-

## Due libri interessanti



Per approfondire i temi di questo articolo ci sono due libri interessanti. Il primo (già citato nel testo) è un'opera di consultazione, e si intitola:

### Annuario di Diritto delle Tecnologie dell'Informazione

Rivista di legislazione giurisprudenza dottrina bibliografia diretta da Donato Antonio Limone - STET, Torino, 1994, L. 150.000

In due volumi, per quasi millecinquecento pagine, sono raccolte tutte le disposizioni normative europee e italiane in materia di informatica e telecomunicazioni, dalle raccomandazioni e dalle direttive comunitarie fino alle circolari ministeriali e ai regolamenti di un grande numero di enti pubblici. Completano il primo volume ben trecento pagine di giurisprudenza, con sentenze emesse da tutti i gradi della magistratura. Il secondo tomo, di dimensioni molto più contenute, offre alcuni pregevoli saggi e una ricca bibliografia.

Un'opera di grande rilevo, dunque, che può essere indispensabile a chi si occupa dei problemi delle nuove tecnologie. Da sottolineare l'approccio globale alla «digital collision», che mette insieme informatica, telefonia e radio-televisione, secondo una tendenza ancora poco diffusa nel nostro

Paese, come sottolinea l'autore nell'intervista pubblicata in queste pagine.

Non meno interessante, anche se di taglio completamente diverso, il secondo libro che non dovrebbe mancare nella biblioteca dei cultori dell'informatica:

### La tutela giuridica dei programmi per elaboratore nella legge sul Diritto D'autore

Giuffrè editore, Milano, 1994, L. 24.000

L'opera ha un deciso taglio giuridico, ma evidentemente l'autrice non ha pensato solo agli addetti ai lavori, perché ha inserito un'ampia serie di riferimenti che consentono di seguire il discorso anche a chi non abbia una preparazione molto approfondita nel campo del diritto. Nella prima parte sono riportati i lineamenti del diritto d'autore prima del DL 518, con le convenzioni internazionali e la direttiva europea 250/91 e un esame della legge 633/41. Si analizzano in profondità, nella seconda parte, gli aspetti giuridici del software, le difese e le sanzioni civili e penali, il ruolo della SIAE e gli aspetti tributari. In appendice i testi completi delle norme del Codice Civile sulla materia, la legge 633/41 aggiornata, il DL 518/92 e la Direttiva europea 250/91.

dere forme di protezione adeguate. Questo non impedisce che chiunque possa partecipare a un chat o a una conferenza usando uno pseudonimo, ma la sua reale identità deve essere conosciuta dal gestore del sistema. Questi può essere vincolato a una forma di segreto professionale, con la sola eccezione delle richieste dell'Autorità Giudiziaria. Dunque l'autorizzazione all'accesso in scrittura deve essere concessa dal gestore del sistema solo a chi si identifica in modo certo, inviando la fotocopia autenticata di un documento o in altro modo. È evidente che il gestore non ha alcuna responsabilità se il richiedente invia una documentazione falsa, a meno che la falsità non sia riscontrabile usando la normale diligenza.

All'identificazione di chi trasmette messaggi (pubblici o privati) segue la logica conseguenza di una documentazione degli accessi, da realizzare attraverso «log» che devono registrare l'attività dei sistemi. Non è accettabile l'obiezione di chi afferma che un log su supporto magnetico è facilmente falsificabile (e sarebbe troppo oneroso, per le strutture senza scopo di lucro o di piccole dimensioni, imporre la registrazione su dischi WORM): anche i registri di carta sono falsificabili, ma le informazioni che contengono sono considerate attendibili fino a quando non viene provato che sono false. La legge 547/93, articolo 3, ha inserito nel codice penale l'art. 491 bis, che recita: *Se alcuna delle falsità previste dal presente capo* (Della falsità in sigilli, strumenti o segni di identificazione, certificazione o riconoscimento) *riguarda un documento informatico, pubblico o privato, si applicano le disposizioni del capo stesso, concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati a elaborarli.*

L'identificazione, senza eccezioni, di chiunque acceda ai sistemi e la registrazione degli accessi sono le prime armi per prevenire i reati telematici. Dunque ogni abbonato a un BBS dovrebbe avere una password, della cui segretezza e del cui uso sarebbe responsabile, insieme al gestore. Questi dovrebbe comunicare anche il livello di segretezza della password stessa. Chi si serva di una password «falsa» compie un reato previsto dagli articoli 615 ter e quater del codice penale (ancora la legge 547/93).

### **Sicurezza e libertà**

Queste norme non bastano a risol-

## **Un decalogo per i BBS**

Ecco, in dieci punti, le norme che potrebbero regolare l'esistenza dei BBS e che potrebbero essere inserite nella futura legge sulla protezione dei dati individuali.

1. Distinzione per forma giuridica tra: a) sistemi amatoriali senza quote di iscrizione, completamente liberi; b) sistemi amatoriali con quote di iscrizione, soggetti alla normativa sui circoli culturali; c) sistemi a pagamento, regolamentati come ditte commerciali.

2. Distinzione per i contenuti tra: a) messengerie private, soggette alle norme sulla corrispondenza privata; b) messengerie pubbliche, soggette alle norme sulla stampa, con nomina di un direttore responsabile (che non deve necessariamente essere un giornalista, ma può essere iscritto all'elenco speciale dei direttori di pubblicazioni tecniche).

3. Classificazione dei livelli di sicurezza delle password e della segretezza dei messaggi privati.

4. Obblighi per i gestori: a) notifica al (futuro) Garante dei dati individuali (esclusi i BBS puramente amatoriali); b) indicazione, in un apposito banner e/o nel contratto di abbonamento, dei dati indicativi della struttura e del suo responsabile, e dei livelli di sicurezza; c) identificazione certa (fotocopia autenticata di un documento o altro) dell'identità degli abbonati; d) documentazione degli accessi tramite «log».

5. Divieto, per i gestori, di leggere i contenuti delle messengerie personali e responsabilità civile e penale dei direttori per i contenuti delle aree pubbliche, nel caso di mancata identificazione dei mittenti (per questo bastano le leggi vigenti, ma è necessario spiegare in un banner che ogni abbonato è responsabile di quanto deposita nelle aree pubbliche).

6. Divieto di accesso in scrittura a chi non sia stato preventivamente identificato dal gestore, ferma restando la facoltà di usare pseudonimi nei messaggi; in questo caso il gestore può rivelare l'identità degli abbonati solo all'Autorità Giudiziaria. L'accesso in sola lettura può essere liberamente regolato dal gestore.

7. Divieto di creazione di messengerie «segrete», ferma restando la facoltà di riservare determinate aree a particolari categorie di utenti.

8. Divieto di sequestro di apparecchiature utilizzate anche per attività non illegali.

9. Obbligo, in caso di perquisizioni, di impiego di personale specializzato o di consulenti qualificati iscritti in appositi registri dell'Autorità Giudiziaria.

10. Regolamentazione, da inserire in una revisione del DL 518, dei diritti sul software di pubblico dominio, shareware e freeware. Depenalizzazione delle infrazioni più lievi alla legge sul diritto d'autore.

# Le opinioni dei giuristi

## Savoldelli Pedrocchi: bisogna rivedere le norme

vere tutti i problemi della sicurezza dei sistemi telematici, compresi i BBS, ma possono rendere più difficile la commissione di atti illeciti attraverso i sistemi stessi.

Ripeto, non è un problema di autorizzazioni di polizia: un BBS amatoriale è come un'associazione e nel nostro Paese i cittadini hanno diritto di associarsi liberamente, senza autorizzazione, per fini che non sono vietati ai singoli dalla legge penale (art. 18 della Costituzione). A tutela della riservatezza dei dati individuali, la legge che deve urgentemente essere emanata potrà stabilire il divieto di diffondere notizie sugli abbonati, con l'eccezione dei loro nomi o pseudonimi. Ma qui torniamo ai problemi *de iure condendo*, alle norme che mancano.

La futura legge sulle banche dati dovrà contenere anche disposizioni che obblighino i gestori a comunicare i livelli di protezione dei sistemi: se le password sono trasmesse o archiviate in chiaro o crittografate, se l'algoritmo di crittografia è reversibile o no, e via discorrendo (ne parla Paolo Nuti nell'editoriale di questo mese).

Un altro punto che deve essere regolato è quello relativo ai sequestri: nei casi di perquisizioni per violazioni alla legge sul diritto d'autore o per reati informatici deve essere sequestrato solo ciò che costituisce specificamente oggetto o mezzo di reato, a meno che non si tratti di sistemi palesemente impiegati o impiegabili solo per scopi illeciti.

Sono problemi che non riguardano solo i BBS, amatoriali o commerciali, ma qualsiasi archivio informatico, qualsiasi sistema telematico. Per questo non credo che sia opportuno richiedere una legge specifica per i BBS, che oggi potrebbe essere solo limitativa della loro libertà. Bisogna insistere perché tutte le attività di questo settore vengano regolate in un quadro legislativo globale, che riveda il DL 518, completi la legge 547 e stabilisca le norme per le banche dati, la protezione della *privacy* e la sicurezza dei sistemi.

Prima di tutto, la futura legge dovrà chiarire definitivamente la natura e i limiti dell'attività di tutti i tipi di strutture telematiche e gli obblighi dei gestori, in modo che sia facile distinguere le persone oneste dai mascalzoni, le attività innocue o utili da quelle dannose per gli interessi della collettività. Ma, accanto ai diritti sulla riservatezza dei dati individuali, deve anche sancire, per tutti, la libertà di trasmettere, di «fischiarne nei fili», di esprimere le proprie opinioni secondo il dettato dell'articolo 21 della Costituzione.

*Il Procuratore della Repubblica di Pesaro, l'ormai famoso dottor Gaetano Savoldelli Pedrocchi, non si aspettava tanto clamore per quella che era partita come un'inchiesta simile a tante altre. E, anche per fermare il diffondersi di voci sempre più fantasiose, ha convocato una conferenza stampa. Insieme al colonnello della Guardia di Finanza Vincenzo Letterese, che ha condotto le indagini, il 17 giugno il Procuratore ha raccontato tutta la storia e ha risposto alle domande dei giornalisti.*

*Alcune domande non hanno avuto risposta, perché l'inchiesta continua e molte informazioni sono protette dal segreto istruttorio. La sensazione è che dietro all'operazione «Hardware 1» ci sia qualcosa di più grave della duplicazione abusiva di software: forse non a caso il Procuratore ha insistito più sugli aspetti di violazione della privacy che sulle copie illegali dei programmi.*

*Ecco alcuni stralci del suo lungo discorso. Che si è rivelato una bella lezione di diritto e anche di buon senso, e ha messo in luce con grande chiarezza i limiti dell'attuale legislazione e alcune possibili soluzioni.*

Nell'indagine, quello che ci preoccupava di più era la possibilità, non solo di violazioni del diritto d'autore, ma di introduzioni abusive nella posta telematica. Quindi una violazione di questa *privacy* così nuova e così stupefacente, per il modo in cui questo mondo nuovo, questa cultura nuova, questo modo di comunicare nuovo si sono diffusi. Anche le conversazioni telematiche a livello personale devono essere tutelate, oltre agli interessi patrimoniali, e quindi abbiamo cercato di individuare se nell'ampio giro degli utenti, degli appassionati e dei professionisti del computer ci fosse stato e ci sia qualcuno dedicato a questa attività. Questa materia per me è un po' magica, io appartengo a una generazione che considera un po' magico tutto questo, non fantascientifico, ma certo affascinante. Altre indagini prima di questa, in altri luoghi, hanno dimostrato che c'è questa possibilità. C'è chi fa il pirata per gioco e c'è chi fa il pirata per lucro, e noi vogliamo colpire chi lo fa per lucro, naturalmente, ma dobbiamo impedire che si fac-



Gaetano Savoldelli Pedrocchi.

cia anche per gioco, perché lo spionaggio, la curiosità del voyeur o dell'ascoltatore abusivo sono invasivi della libertà personale. Quindi lo scopo di questa indagine non è di limitare la libertà di informazione, la libertà di comunicazione, né le possibilità future di un'estensione sempre maggiore della libertà. Il fine è l'opposto: tutelare questa libertà proprio nell'individualità di chi ha diritto alla sua *privacy*, ai suoi diritti commerciali e ai suoi diritti di autore. Questo è lo scopo di questa indagine.

**Però, condurre perquisizioni a tappeto in abitazioni private, sigillare camere da letto, interrompere reti di comunicazione che svolgono anche attività del tutto legittime, non è un po' troppo?**

**Bisogna anche dare conto dell'inesperienza, perché quella del computer è una tecnica e una cultura. Una tecnica molto diffusa, anche nei nostri uffici ci sono apparecchi che chiamiamo computer, anche se in realtà non svolgono ancora questa grande funzione. La cultura del computer è ben diversa dall'aspetto meramente tecnico di utilizzare una memoria. E quindi do atto che anche noi, con la necessità di operare contemporaneamente (perché queste cose viaggiano alla velocità della luce e gli uomini sono molto lenti nel seguirle), siamo stati costretti ad agire contemporaneamente con molti comandi, grandi e piccoli. In molti casi i comandi si sono**

avvalsi di esperti della Guardia di Finanza, dove era possibile, in alcuni altri si sono avvalsi di tecnici estranei al Corpo e in qualche caso c'è stato un pochino di grossolanità nell'intervento, questo sono il primo ad ammetterlo. Però abbiamo cercato di rimediare velocissimamente. Danni ne abbiamo provocati, abbiamo cercato di eliminarli il più presto possibile, e stiamo restituendo in uso le macchine, cercando di assicurare in modo serio le prove senza interrompere le reti e neppure impedire i giochi dei bambini.

**Nelle vostre indagini avete trovato aree di illegalità in enti pubblici o in istituti universitari?**

**Ma** gli istituti di ricerca e universitari sono poverissimi! Come possono accedere al mercato se non arabbattandosi un po'? Questo fa parte della povertà della ricerca italiana, poi si sa, tra ricercatori... Sono cose, tutto sommato, innocenti.

Lo studente che deve scrivere la tesi, come deve fare? Io non voglio drammatizzare questo aspetto, perché ogni illecito va perseguito, ma gli studenti si sono sempre fotocopiati e passate anche le dispense col diritto d'autore del professore!

**Dottor Savoldelli, vorrei porre una domanda al giurista, al di fuori di questa indagine. Le pensa che una revisione della 518, che molti richiedono, dovrebbe tener conto di questi aspetti?**

**Credo** che la scienza di questa materia

abbia in un certo senso sfondato una frontiera, non siamo più entro i limiti del controllabile e del gestibile secondo una normativa che attenga meramente alle condotte. La tecnologia ha sfondato una frontiera e adesso fa i conti con se stessa. Occorre che sia la stessa tecnica, la scienza, a venire incontro alla legge e proponga dei rimedi oggettivamente realizzabili per la difesa di qualche cosa che altrimenti non è difendibile. Vediamo il diritto d'autore: per esempio, nel campo della moda le grandi firme hanno un tempo di alcuni mesi prima di essere imitate e copiate, per cui possono realizzare i profitti dei loro investimenti in poco tempo, la moda diventa subito di dominio pubblico. Ma anche l'autotutela io la vedo male, in molti casi non credo che sia accettabile. E allora, secondo me, nella riforma della 518 si deve considerare che l'eventuale uso illecito per motivi che non sono di lucro (anche se c'è un piccolo profitto, quello dello studente che invece di comperare, copia) dovrebbe essere considerato a parte. Dovrebbe scadere dal reato di ricettazione, che viene proposto attualmente come se fosse un reato da niente, ma che per la legge è un reato più grave della copia abusiva.

**Tra associazione a delinquere e ricettazione, un gruppo di studenti che copia un software per fare una tesi può essere condannato a parecchi anni di galera!**

**La legge prevede come un reato non gravissimo la duplicazione abusiva, ma**

la ricettazione arriva molto più in là. Quindi si dovrebbe fare una norma speciale che punisca, ma con una contravvenzione, con una sanzione amministrativa, il possesso indebito non a scopo di lucro né di diffusione. Invece ritengo che debbano essere punite le violazioni della privacy forse in maniera molto più forte di quello che ha previsto la riforma del codice penale fatta con la 574, perché quelli sono reati estremamente gravi. Ma, ripeto, ritengo che dobbiamo proteggere al massimo la libertà di comunicazione e di espressione, e nello stesso tempo al massimo della segretezza. Penso che nella riforma si debba individuare una norma che sia eccezionale rispetto alla legislazione, una norma speciale, perché venga meglio individuata la pericolosità dell'invasione della sfera privata nella posta telematica.

E naturalmente bisogna difendere anche gli interessi economici, molto importanti, che non sono solo quelli dei produttori, ma degli enti pubblici, delle banche...

**In conclusione, dottor Savoldelli?**

**Posso fare una confessione?** Questa è una specie di vendetta del computer, perché tutto questo è capitato in una struttura il cui titolare si serviva dei collaboratori anche per un piccolo movimento sulla tastiera.

È una specie di vendetta, che mi ha costretto ad entrare in una materia affascinante. Prometto che d'ora in poi cercherò di capirne personalmente di più.

## D'Aietti: i limiti del sequestro

*Il giudice Gianfranco D'Aietti, della Corte d'Appello di Milano, è un grande esperto di informatica, ed è stato tra i primi magistrati italiani dei diritti d'autore sul software. Alcune sue sentenze hanno costituito precedenti importanti prima del DL 518/92.*

\*\*\*

**Dottor D'Aietti, l'azione penale della Procura di Pesaro contro alcuni pirati informatici ha portato al sequestro di intere banche dati e al blocco parziale di una rete telematica. Non è un po' troppo?**

**Il problema dei sequestri penali non si**



Gianfranco D'Aietti.

può risolvere in due parole, soprattutto se si tratta di sequestri di tipo preventivo, ossia rivolti ad impedire che gli oggetti possano essere utilizzati per commettere ulteriori reati. Nel campo dei sequestri probatori, cioè di quelli che servono per accertare la sussistenza del reato, esiste già nella legge il principio che se le cose non sono più necessarie ad ottenere la prova, le stesse vanno restituite all'avente diritto. Certo è che quando si sequestrano sistemi telematici, che hanno funzioni di comunicazione, occorre procedere con particolare cautela in quanto, in seguito alla quasi completa equiparazione attuata dalla recente legge 547 del '93 delle comunicazioni telematiche alla corri-

spondenza, si pongono sul punto i medesimi limiti, particolarmente delicati, del sequestro della corrispondenza. Per esempio, in materia fiscale ci sono norme che escludono la possibilità di sequestrare i libri contabili. Quando si fanno dei sequestri di tipo fiscale-tributario, la Guardia di Finanza non può sequestrare i libri contabili su cui l'azienda deve fare le sue contabilizzazioni e deve lavorare: può semplicemente apporre dei sigilli, a delle parti ben precise, per evitare scritturazioni successive, oppure può acquisire i dati interessanti l'indagine.

Questa dovrebbe essere la tecnica di indagine quando si opera in una struttura che ha una sua vita autonoma, che non può essere bloccata solo per accertare un reato.

Oppure lo si può fare per il tempo strettamente necessario a esaminare il materiale, con un'accortezza tecnica tale da «fotografare» la situazione, e poi lasciare libero il soggetto di continuare tutte le attività che non sono illecite.

**È la soluzione, mi pare, che lei ha applicato in un caso celebre, quello della causa intentata alcuni anni fa dalla Microsoft contro un'azienda che vendeva il DOS copiato abusivamente.**

**Certamente.** In quel caso, si trattava di una causa civile, ho emesso un decreto di sequestro dei computer sui quali si fosse trovato il software illegale, e di immediato dissequestro, subordinato alla rimozione dei programmi riprodotti illecitamente, applicando l'articolo 159 della legge sul diritto d'autore, che prevede la separazione tra l'opera illecitamente riprodotta o diffusa e le apparecchiature impiegate, nel caso che servano anche per altre attività.

**Ma si trattava di una causa civile, perché allora copiare il software non era previsto come reato. Lo stesso criterio può essere seguito in campo penale?**

**Se i reati contestati sono solo quelli previsti dal DL 518/92 sulla tutela dell'opera di ingegno, poiché nella legge sul diritto d'autore vi è un collegamento molto stretto tra i poteri di tutela in via civile e in via penale. In quel caso i poteri che la legge concede al giudice penale per assicurare la tutela del diritto leso sono espressamente quelli previsti in via civile.**

**In questo caso sono state contestate anche violazioni alla legge 547/93, come l'accesso abusivo a sistemi informatici.**

**Allora il discorso diventa più ampio,**

non ci sono i limiti dell'articolo 159. Nel caso di violazione della 547, computer e modem diventano mezzi per la commissione del reato e quindi possono essere soggetti a confisca quando la sentenza passa in giudicato. E anche nell'ambito della 518 ci potrebbero essere esigenze di accertamento che potrebbero ampliare il sequestro al di là dei limiti dell'articolo 159 della 633, che può servire come riferimento per determinare gli interessi in gioco, però sempre con finalità di accertamento probatorio, in considerazione di aspetti particolari.

\*\*\*

*Ed ecco i punti più interessanti del decreto stilato da Gianfranco D'Aietti, allora pretore di Monza, nel 1988 (pubblicato ne «Il diritto dell'informazione e dell'informatica» n. 1/1989, ed. Giuffrè).*

[...] Ai sensi della legge sul Diritto d'Autore, il sequestro può avere ad oggetto (ai sensi del combinato disposto degli artt. 161 e 159) ciò che si ritenga in violazione del diritto di utilizzazione ovverossia (art. 159) «gli esemplari o copie illecitamente riprodotte o diffuse, nonché gli apparecchi impiegati per la loro diffusione che, per loro natura, non possono essere adoperati per una diversa riproduzione o diffusione».

Orbene il sequestro ben può essere disposto per i programmi registrati su floppy disks e duplicati abusivamente; per essi si verte nel settore del diritto d'autore e della relativa tutela.

Il sequestro può anche estendersi alle copie del sistema operativo MS-DOS registrate su disco fisso (contenuto fisicamente all'interno dei computers) sui quali il sistema operativo sia stato installato proveniente da una copia abusiva. In tali casi può essere disposto il sequestro dell'intera apparecchiatura in cui sia stato installato il sistema operativo MS-DOS.

Occorre notare che, però, mentre nessun dubbio vi potrà essere, in sede di sequestro, in ordine alle copie abusive registrate su dischetto magnetico (c.d. floppy disk), seri dubbi possono aversi sulle copie installate su «disco fisso»: infatti tali registrazioni sono, per definizione, delle «copie» che possono provenire sia dai floppy disk originali della Microsoft Corporation sia da copie abusive.

Di conseguenza occorre precisare adeguatamente i limiti entro cui può operarsi il sequestro delle copie illecitamente contraffatte registrate sui dischi fissi; il criterio non potrà essere che quello di verificare, per ciascuno dei dischi fissi rinvenuti nei locali della Melchioni Computertime SpA, se la presenza di un sistema operativo MS-DOS sia ricollegabile a una confezione originale della Microsoft Corporation che sia stata dissigillata ed il contenuto sia, verosimilmente, stato copiato (legittimamente) sul disco fisso. Nel caso in cui, in sede di sequestro, invece, si sia in presenza di un disco fisso con installa-

to un sistema operativo MS-DOS e non sia presente, invece, la confezione originale della Microsoft Corporation (dissigillata) si potrà procedere al sequestro del relativo computer ove è contenuto il disco fisso.

Parimenti il sequestro non potrà essere operato in tutti quei casi in cui il disco fisso dei computer, come evidenziato dalla stessa ricorrente, sia stato installato all'origine in base a un apposito contratto di licenza stipulato tra la Microsoft Corporation e il produttore del computer (nel qual caso la licenza è «incorporata» nella versione di MS-DOS installata sul disco fisso).

Poiché viene autorizzato il sequestro degli «apparecchi utilizzati per la riproduzione» (art. 159, comma 1) dell'opera di ingegno abusivamente riprodotta, fin d'ora può prevedersi il dissequestro delle apparecchiature hardware, in cui fosse installato il sistema operativo MS-DOS, in applicazione della norma di cui all'art. 159, comma 2, che prevede che «se una parte... dell'apparecchio di cui si tratta può essere impiegata per una diversa riproduzione o diffusione, l'interessato può chiedere a sue spese la separazione di questa parte nel proprio interesse».

Orbene, appare evidente che il sequestro dei dischi fissi appare funzionale solo rispetto alla tutela dell'opera di ingegno «programma operativo per elaboratore» e che, attuata la tutela prevista dalla legge, il mantenimento del sequestro sarebbe solo un danno ulteriore e non ulteriormente giustificabile nei confronti della Melchioni Computertime SpA, qualora questa fosse intenzionata ad eliminare l'abusiva riproduzione dai dischi fissi.

La legge prevede esplicitamente tale ipotesi ed appare opportuno fin d'ora dare attuazione a tale previsione disponendo il dissequestro delle apparecchiature hardware sequestrate, dischi fissi e relativi computer che li contengono, qualora la Melchioni Computertime SpA richieda la «separazione» del sistema operativo dalle apparecchiature. Tale separazione dovrà avvenire attraverso la eliminazione fisica completa del sistema operativo MS-DOS dai dischi fissi e relativi supporti attraverso un procedimento tecnico efficace che sia verificato dal perito che viene contestualmente nominato nel presente decreto.

[...] All'esito delle operazioni del perito, che avrà attestato formalmente che il sistema operativo sia stato definitivamente cancellato dai dischi fissi, i relativi supporti fisici potranno intendersi dissequestrati senza ulteriore formale provvedimento di questo giudice, bastando a tale scopo la attestazione dell'ufficiale giudiziario [...].

*Questa è la parte più importante del decreto di D'Aietti, che contiene nello stesso tempo l'ordine di sequestro del computer, l'esecuzione della richiesta di cancellazione del software copiato illecitamente, e il successivo, immediato dissequestro.*

*Nelle azioni penali per la violazione del copyright, si dovrebbe applicare lo stesso criterio, con una piccola variante per l'acquisizione della prova del reato: prima della cancellazione si dovrebbe procedere alla copia del software con-*

tenuto nell'hard disk. L'ufficiale di polizia giudiziaria che opera la perquisizione attesterebbe che la copia riproduce esattamente il contenuto del disco rigido e dissequestrerebbe immediatamente

il computer. E se sul momento non fosse possibile fare la copia, si potrebbe sequestrare solo il disco rigido, per il cui smontaggio bastano pochi minuti e una minima competenza tecnica.

Resta però un punto fondamentale: queste azioni dovrebbero essere sempre affidate a personale dotato di una preparazione specifica, o con l'intervento di un perito nominato dal giudice.

## Coliva: troppi pregiudizi sulla telematica

L'avvocato Daniele Coliva difende alcuni degli indagati dalla Procura di Pesaro. Il giovane penalista bolognese è un informatico esperto e appassionato, e quindi si sente particolarmente coinvolto nella vicenda: al Tribunale del riesame ha detto «Non capisco, a questo punto, perché non sono stato perquisito anche io». Perché?

\*\*\*

**A**vvocato Coliva, perché avrebbero dovuto indagare anche su di lei? C'è qualcosa che non funziona nell'inchiesta?

A mio avviso il problema non è del tutto chiaro anche alla luce delle informazioni che, come difensore, avevo avuto modo di conoscere in precedenza. Dal punto di chi deve progettare e mettere a punto una strategia difensiva rimangono molti dubbi su quali siano effettivamente i presupposti di fatto sulla base dei quali l'indagine è nata ed è stata portata avanti, attraverso strumenti molto penetranti come la perquisizione e il sequestro.

Per un verso mi sembra di poter dire che ci sia stata una carenza di informazione, di conoscenze, da parte di chi ha svolto un'indagine sulle banche dati amatoriali e sulle loro modalità di funzionamento e di collegamento, e per un altro mancano ancora troppi elementi per capire bene i contorni dell'azione penale.

In effetti il Pubblico Ministero non ha detto tutto, si è limitato a pochissime cose, e per questo in chi difende restano sempre la cautela e il dubbio che non ci siano in realtà gli altri elementi più concreti e più importanti, che non verrebbero svelati perché l'indagine è ancora in corso.

Un'indagine, è sembrato di capire nella conferenza stampa, che adesso procede in modo diverso da come è iniziata.

Non so se fino a ora l'indagine non sia stata fatta così a colpo sicuro, cioè se abbia colpito sempre e comunque sog-



Daniele Coliva.

getti coinvolti nei reati contestati al nucleo di indagati di Pesaro, perché il Tribunale del riesame da questo punto di vista ci ha dato ragione. Infatti in un primo momento ha detto che non aveva elementi per controllare il «fumus boni iuris», perché la Procura non aveva fornito abbastanza elementi di giudizio, ma quando la Procura ha detto di più, comunque si è sempre rimasti su affermazioni probabilistiche, molto poco delineate, che non sono state ritenute sufficienti per mantenere la cautela sul materiale sequestrato.

Tutto quello che rimane ancora sotto sequestro è solamente il software, perché ritenuto, in ipotesi, confiscabile obbligatoriamente, e quindi soggetto a divieto normativo assoluto di dissequestro.

Se non ci fosse stato questo, se il software non fosse corpo di reato, sarebbe stato dissequestrato.

**S**otto qualche aspetto sembra di capire che, almeno inizialmente, si siano mossi partendo dall'assunto che una persona che ha un modem è un pirata, o che sia un malfattore telematico perché si è collegato con un'organizzazione dedicata a traffici illegali. Secondo lei, è possibile?

È possibile. Anzi, da alcuni elementi oggettivi che si colgono dall'indagine,

la conclusione è che si è portati a prendere è proprio questa: cioè che in realtà si sia indagato solo sulle base dei collegamenti in partenza dall'organizzazione pesarese.

Mi pare di averlo detto in una udienza del riesame, che probabilmente quelli di Pesaro hanno agito come tanti untori che hanno infettato banche dati qua e là per la penisola, perché, da quanto attualmente consta, il controllo è stato effettuato su chiamate in uscita da Pesaro ad altre banche dati. Però non si sa nulla sul contenuto di questi collegamenti, né è francamente ipotizzabile uno smercio di software attraverso il modem, per le dimensioni attuali dei programmi, che rendono assolutamente antieconomico uno strumento di questo genere. D'altra parte, a mio avviso, non è possibile, non è logicamente credibile e giuridicamente sostenibile che questi collegamenti, di cui si può intravedere solo la modestia quanto a dimensione quantitativa, possano essere ritenuti il fondamento di un'imputazione di associazione per delinquere. Cioè di un'organizzazione, e un'organizzazione non si ricostruisce sulla base di collegamenti telefonici unidirezionali. Ma il problema è che si vede ancora l'informatico con il modem, l'informatico in collegamento col mondo, come un soggetto esoterico, un esoterista in possesso di cognizioni particolari, che lo rendono anomalo, un diverso, e quindi da controllare, da sorvegliare.

Il problema è questo. E ce n'è un altro, molto delicato, che è rappresentato dalla normativa sul software. Essa può diventare, di fronte a questo pregiudizio, un pregiudizio sull'informatico-telematico.

La normativa sul software può diventare uno strumento di scardinamento della telematica a qualunque livello, soprattutto amatoriale, perché attraverso le possibilità di indagine e di intervento violento come sono perquisizione e sequestro, è possibile azzerare un'attività telematica sulla base di semplici sospetti.

## Limone: manca il quadro globale

*Donato A. Limone, docente di Informatica Giuridica all'Università di Camerino, è l'autore dell'Annuario di Diritto delle Tecnologie dell'Informazione, edito dalla Seat. Sono circa millecinquecento pagine di norme europee, nazionali e regionali, raccomandazioni, regolamenti, insomma un «corpus iuris» completo sul diritto dell'informatica (a proposito, perché un libro e non un più pratico CD-ROM?).*

\*\*\*

**P**rofessor Limone, nella prossima edizione del suo Annuario ci sarà anche la legge sulle banche dati? E, secondo lei, dovrebbe regolamentare anche l'attività dei BBS?

**Q**uello che occorre è un minimo di legislazione pianificata, coerente e integrata, perché ormai anche i media non possono restare fuori da questo discorso. Almeno tendenzialmente, non subito, ma la prospettiva è questa. E allora il legislatore deve pianificare: se mancano le norme sulla privacy e le banche dati, non si deve pensare che questo non abbia niente a che fare con le telecomunicazioni e i mass media. Intanto si può legiferare su questo punto, ma quando si integreranno i nuovi media con la televisione, inevitabilmente il problema si riproporrà. La legislazione deve essere di tipo pianificato, coerente e integrato anche con altri sistemi di comunicazione. Si può fare anche una legge sui BBS, si può anche legiferare in modo settoriale, se serve, però si deve avere davanti agli occhi il quadro generale, ed è quello che manca.

**Il nuovo Parlamento lo sa? Potrebbero esserci interessi particolari a frenare l'innovazione legislativa?**

**Il** mondo si sta integrando tecnologicamente e i legislatori dovrebbero fare nello stesso modo. Ma non lo fanno, non c'è niente da fare. Il legislatore non sa che deve comportarsi in un certo modo, non pianifica in nessun campo, almeno in questi settori strategici. In questo modo va contro la collettività, quindi figuriamoci se può avere un interesse. Dovrebbe avere l'interesse a pianificare bene per aumentare tutto il discorso del mercato, potrebbe potenziare nuovi comparti tecnologici, come l'integrazione della telefonia con tutto il



Donato A. Limone.

resto, potrebbe pianificare anche lo sviluppo di professioni e di occupazioni. C'è da fare tutto un discorso nuovo sui servizi, ma la logica resta quella tradizionale, quella arcaica: io ti fornisco il servizio del telegramma e tu mi paghi il servizio dei telegrammi, senza considerare che il telegramma può essere un servizio superato o integrato da altri. Noi oggi siamo in questa situazione, stiamo uscendo dal monopolio delle telecomunicazioni, dove SIP faceva da gestore, faceva da information provider, faceva di tutto, mentre le direttive europee dicono che un conto è gestire le reti e un conto fornire i servizi a valore aggiunto, che devono essere liberalizzati. Allora, se questo è vero, vuol dire che il legislatore non può più andare avanti stabilendo semplicemente le tariffe per servizi o per singoli segmenti di servizi, senza avere un quadro generale. Si deve partire dall'idea che questo è un settore strategico, sul quale si deve investire pesantemente, non per fare arricchire le aziende del settore con banali strumenti tariffari, ma perché si può incrementare il mercato del lavoro, si può dare lavoro alla gente, fornire servizi migliori alla collettività, accrescere la qualità delle professioni. Questo significa legiferare, oggi, in un'Europa moderna. E tutto questo in Italia manca.

**Nonostante le dimensioni di questo Annuario...**

**L'**Annuario segue la logica di vedere le tecnologie in modo integrato, enfatizzando il declino dei monopoli. Solo attraverso il declino dei monopoli si può liberalizzare: è la politica dell'Unione Europea, della Thatcher. Non ha caso la

Gran Bretagna, che ha liberalizzato le poste e le telecomunicazioni in modo veramente molto forte, è più avanti di tutti in questo settore. Quando gli inglesi si sono posti il problema di come condurre strategicamente il cambiamento, se lo sono posti in modo complessivo.

Si sono chiesti che cosa significasse la liberalizzazione dal punto di vista dell'economia generale, dei servizi, del mercato del lavoro, dello sviluppo dell'industria, si sono dati una risposta e sono partiti. Invece noi non ci siamo dati nessuna risposta, abbiamo detto: dobbiamo privatizzare i servizi ed eliminare i monopoli, che facciamo? L'azienda di Stato la dobbiamo eliminare, dobbiamo sistemare una società delle poste... sono politiche che seguono logiche settoriali. Se andiamo a vedere atti parlamentari, direttive, decreti e quant'altro, che hanno riformato questo settore, si può toccare con mano questo modo atomizzato di legiferare, senza una linea direttrice, senza una pianificazione. In questo modo il diritto, che potrebbe dare una grossa spinta al cambiamento tecnologico e alle strategie del mutamento sociale, invece frena, e frena in modo pesante.

**E frena anche la telematica amatoriale...**

**E** non solo, perché quello delle tecnologie è un settore strategico. Attenzione, se lo si frena si perde il treno e si diventa debitori verso gli altri paesi, quindi l'innovazione tecnologica costa di più, si diventa una colonia, un Paese di serie B. Non ci possiamo permettere di sbagliare, altrimenti rimaniamo debitori di tutto verso gli altri Paesi. Non è solo un problema di materia prima, ma è la materia prima delle materie prime, l'informazione, senza la quale non c'è sviluppo.

Questa logica di integrazione non c'è, non l'ho creata io con questo volume, mi sto sforzando di mettere insieme i materiali e dire al legislatore: cerca, da oggi in poi, di dare un po' di corpo a questa materia, che è disorganica. Altrimenti restiamo fuori da tutto il discorso di Clinton, da tutto il discorso di Delors, per restare in ambito europeo. Sulle autostrade elettroniche, chi arriva un minuto dopo è fuori gioco, questo è il discorso che il legislatore non vuole capire.

MS

technologies  
**TEN**



TAIWAN



ITALIA

**logica soluzione**  
al problema dell' approvvigionamento

Salvaguarda ed accresci i tuoi utili importando direttamente da Taiwan, Hong Kong, Singapore e Cina.

Acquista con interlocutori italiani sul posto.

- ◆ Un organizzazione consolidata per un servizio door to door dall' Oriente.
- ◆ Garanzia del prodotto direttamente dall' Italia.
- ◆ 600.000 sistemi TEN TECHNOLOGIES operanti nel mondo

- Green-PC Board
- PCI, Local Bus, ISA
- Hard Disk
- Memorie
- CPU

**TEN**

ITAICO CO.,LTD - Room, #4, 3RD FLOOR  
112 CHUNG SHAN N. RD., SEC. 2,  
TAIPEI, TAIWAN, R.O.C.

Tel. 00886 / 2 - 5516248  
Fax. 00886 / 2 - 5516201

OLITEAM spa  
Via Diaz 28,  
28010 CAVAGLIO D'AGOGNA (NO) I

Tel. 0322 / 806606  
Fax 0322 / 806586  
BBS 0322 / 806624