Considerazioni su alcuni fatti di cronaca

Delinquenza reale, terrorismo virtuale

Software copiato o software contraffatto, «Falange armata» o perditempo telematici, l'informazione che perde colpi e non riesce a far capire alla gente che cosa sta veramente accadendo: è necessario cercare di chiarire il significato di alcuni recenti episodi, al di là della cronaca quotidiana

di Manlio Cammarata

Un tempo i cronisti di nera iniziavano la giornata scorrendo il «mattinale» della Questura, che riportava i fattacci della notte appena trascorsa, e spesso concludevano il lavoro facendo il giro dei reparti di pronto soccorso degli ospedali. Oggi è tutto su un monitor: le notizie d'agenzia, la posta elettronica, i «newsgroup» di Internet. Le informazioni che prima bisognava andare a prendere, letteralmente, con le mani e coi piedi, oggi arrivano sotto forma di bit. Una parte di queste notizie non è cambiata: furti, omicidi, risse, atti osceni in luogo pubblico, incidenti di ogni tipo. Ma ce ne sono altre del tutto nuove, come gli arresti dei pirati del software, gli «atti osceni in rete», le intrusioni nei sistemi telematici e altro ancora.

Il cronista, lo sguardo fisso sul monitor, spesso non ci si raccapezza. Un morto è un morto, una persona scomparsa è qualcuno che non si riesce a trovare. Una violazione di domicilio si verifica, senza dubbio, quando qualcuno entra fisicamente in una casa nella quale non ha il permesso di entrare. Quando viene arrestato un individuo che vende falsi Rolex o la perquisizione in un negozio fa scoprire false borse di Fendi, il reato è chiaro, il dolo è evidente, il reo deve essere identificato, processato e, possibilmente, ospitato per qualche tempo nelle patrie galere. Non è difficile per il cronista dare la notizia, non è difficile per il lettore capire che cosa è accaduto.

Ma quando le forze dell'ordine, al termine di silenziose indagini, arrestano qualche pirata del software, tutto diventa più nebuloso. Quale reato ha commesso costui? Violazione del decreto legislativo 518/92, è la risposta; nel linguaggio comune è un ladro, un ricettatore, uno spacciatore di bit. Bit falsi? No, i bit sono sempre veri, e valgono miliardi di lire. Ma quanto costa un bit, quanto costa un dischetto? Come si fa a rubare miliardi mettendo dei bit sui dischetti? È difficile da capire e da spiegare, è difficile inquadrare la notizia, darle una dimensione che renda l'idea della gravità del fatto.

Le cose si complicano ancora di più quando la notizia riguarda faccende di sesso. Grande scalpore ha suscitato in settembre la notizia che la polizia americana, dopo due anni di laboriose indagini, ha pizzicato dodici figuri, fra i tre milioni di abbonati alla rete Prodigy, dediti all'adescamento telematico di minorenni. È una notizia da sbattere in prima pagina, gridando allo scandalo della pornografia virtuale, o basta un «taglio basso» nelle cronache dall'estero? Proviamo a immaginare lo stesso fatto nel mondo reale: la polizia di Roma indaga a tappeto per due anni fra i tre milioni di abitanti della città, e alla fine identifica dodici pederasti...

Nell'universo tecnologico i fatti si verificano in forme diverse da quelle a cui siamo abituati. La persona che subisce un furto se ne accorge perché non è più in possesso della cosa rubata. Il «furto» di bit, invece, non priva il proprietario dei bit stessi, essi restano al loro posto, e la cosa rubata si trova contemporaneamente in possesso della vittima, del ladro, del ricettatore e di molte altre persone. Occore un salto culturale per comprendere il significato del fatto, e anche il giurista si trova spesso molte difficoltà per classificare il reato tecnologico.

Come interpretare, come raccontare la notizia di qualcuno che «si introduce» abusivamente nel sistema telematico di un altro, in una macchina elettronica, senza che vi sia un passaggio fisicamente percettibile? Sono bit-intrusi che si mescolano a bit-proprietari, gli uni identici agli altri. A volte i primi «feriscono» o «uccidono» i secondi, a volte si limitano a manifestare la propria presenza sotto forma di messaggi inquietanti. Ma a prima vista, nell'incombere dei tempi di chiusura della pagina, come si fa a capire (e a far capire al lettore) che cosa è veramente successo?

Una bomba che esplode tra la gente o accanto a un monumento è quasi certamente un attentato terroristico. Ma un computer che si blocca mentre un messaggio sul monitor dice «questo è un attentato terroristico» è realmente il risultato di un atto di terrorismo? Oppure è l'opera di un imbecille?

Oltre la cronaca

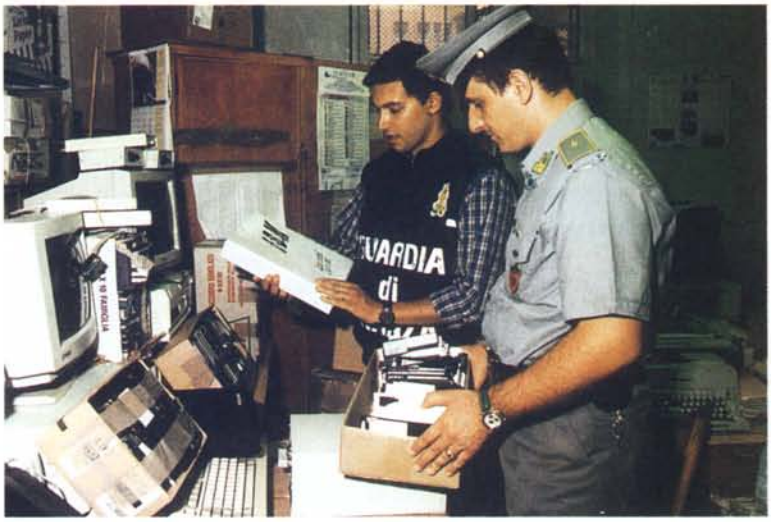
È necessario mettere le cose in chiaro, inquadrare i fatti in un contesto che non sia tracciato solo per attirare il lettore, cercare di spiegarne il

significato e prevederne le conseguenze. Cerco di farlo con queste note, partendo da alcuni recenti fatti di cronaca.

Il primo riguarda un'operazione compiuta dal Nucleo regionale di Polizia Tributaria di Milano, diretta dal procuratore aggiunto Nicola Cerrato, che coordina un pool di magistrati specializzati nella materia. Le Fiamme Gialle, dopo approfondite indagini condotte anche «con l'approccio sperimentale ad intercettazioni telematiche», hanno distrutto un'organizzazione che produceva software falsificato su scala industriale. Impressionante l'elenco dei materiali sequestrati: 25.000 floppy, 210 unità hardware (PC, scanner, schede) quasi 2.000 manuali, 21.000 etichette contraffatte. Il punto interessante è proprio questo: i malfattori, che lavoravano tra la «centrale» di Savona e una dozzina di altre città, non si limitavano a distribuire copie pirata a basso prezzo, ma producevano veri e propri «falsi», riproducendo le scatole originali, i manuali, le etichette e quant'altro. Si trattava quindi di vera e propria contraffazione commerciale, in grado di ingannare perfettamente gli acquirenti. Con una differenza, rispetto alle usuali imitazioni di beni di lusso: che il software falso funziona esattamente come quello vero (se è copiato correttamente). L'utilizzatore lo paga come se fosse vero, e come tale lo usa. Non subisce il danno di quando compera un falso Cartier, che dopo un po' smette di funzionare: con il software falso si riceve quello che si paga con soldi veri.

Chi falsifica il software compie un reato «comune», prima ancora che un reato «informatico», e nel computo degli anni di galera contano più le violazioni classiche del codice penale che quelle punite dal DL 518/92 sulla protezione del software. Ma in questa vicenda c'è un aspetto, sul quale tornerò più avanti, che merita una riflessione: l'impossibilità per l'utente di distinguere il vero dal falso, l'originale dall'imitazione.

Un'altra operazione della Guardia di Finanza (questa volta ad opera della terza Compagnia del II Gruppo di Roma, con la «firma» del sostituto procuratore Giuseppe Corasaniti) rientra invece nella normalità della repressione della pirateria del software, perché il traffico riguardava i soliti programmi copiati abusivamente in quantità. E che quantità: 32.000 dischetti, 1.300 CD-ROM e 56 magneto-ottici sequestrati, oltre al solito corredo di hardware. Il fatto nuovo, e preoccupante, è la presenza di una certa quantità di software specialistico, come le raccolte di giurisprudenza su CD-ROM, che non sono certo prodotti di larga diffusione. Questo significa che c'è una richiesta di software irregolare anche da parte di utenti di alto livello, come gli avvocati, che dovrebbero ben conoscere la natura giuridica della transazione che compiono: ricettazione. Questo deve far riflettere, perché c'è una grande differenza tra il comportamento di un acquirente di software falso (che sembra autentico) in un negozio, e quello di chi compera software palesemente copiato. Nel primo caso si può tranquillamente presumere la buona fede dell'acquirente, nel secondo no. Compera un programma su una bancarella, su dischetti o CD-ROM non originali, senza manuali o con manuali fotocopiati... è solo un «incauto acquirente», o un ricettatore, secondo il disposto dell'art. 648 del Codice penale?



La Guardia di Finanza al lavoro durante un'operazione contro i pirati del software.

Qui vorrei fare una breve digressione giuridica. La contestazione del reato di ricettazione a chi acquista software copiato illegalmente ha suscitato molte perplessità fin dalle prime letture del DL 518/92. Si osserva che in molti casi la pena appare spropositata (fino a sei anni) rispetto al reato principale (fino a tre). Recentemente è stata sollevata, da parte di un difensore di presunti «pirati», l'obiezione che l'art. 648 cp punisce chi «acquista, riceve od occulta denaro o cose provenienti da un qualsiasi delitto», mentre il software non è, per comune opione, una «cosa» (e nemmeno denaro). L'ipotesi difensiva è interessante, ma resta il fatto che chi acquista consapevolmente software irregolare compie un'azione che deve essere considerata illegittima. Probabilmente basterebbe una modifica al 518 per risolvere il problema (compatibilmente con le norme europee), che estendesse all'acquirente le pene previste per chi *abusivamente duplica... importa, distribuisce, vende, detiene a scopo commerciale o concede in locazione* programmi di provenienza irregolare (art. 171 bis). Forse in casi come questi non sarebbe esagerato mettere sullo stesso piano il duplicatore abusivo e l'acquirente in mala fede, e cadrebbe la più grave accusa di ricettazione. Resta il fatto che in molti casi di «copia per uso personale» si dovrebbero prevedere sanzioni molto più lievi, soprattutto quando il «fine di lucro» non sia così evidente o essenziale (il caso classico dello studente che scrive la tesi di laurea con un word processor copiato, ovvero un concetto di «modica quantità»).

Bombe telematiche

Ritorniamo alle cronache, con due fatti molto più preoccupanti e che richiedono riflessioni attente. Domenica 1 ottobre 1995, titoli in prima pagina annunciano che terroristi informatici hanno colpito i sistemi informativi della Banca d'Italia, oltre a quelli di alcune aziende. La Repubblica si distingue per il consueto catastrofismo: «Terrorismo informatico, la Falange all'assalto», ma non dà molte informazioni su che cosa sia realmente accaduto. L'unica notizia certa è che «il loro computer, collegato alla rete Internet, ieri è stato precipitosamente staccato. Più equilibrata e più informata si rivela l'Unità. Titola: «Abbiamo i codici. La Falange armata insidia Bankitalia», ma avverte nell'occhiello: «Messaggio via Internet. Avvertimento o brutto scherzo?». Nel testo si precisa che, secondo la Digos, «uno o più pirati informatici sarebbero effettivamente riusciti a penetrare nell'appendice del sistema di Bankitalia dedicata allo scambio dei dati con la rete delle reti... In ogni caso i sistemi della banca centrale non avrebbero subito alcun danno, neppure temporaneo». Il che riporta la notizia alle sue giuste proporzioni. In realtà il messaggio della sedicente organizzazione terroristica è giunto a molti altri «siti», oltre a quelli citati dalle cronache, ed è subito circolato in rete tra gli addetti ai lavori. Che, dopo un rapido esame, sono stati concordi nel ritenere che, chiunque fosse l'autore dell'azione, non aveva fatto un grande sfoggio di conoscenze tecnologiche, fermandosi in realtà nell'anticamera del sistema. Ma il risultato finale, purtroppo, è esattamente quello previsto dai «terroristi telematici», o sedicenti tali: gettare l'allarme, con la complicità involontaria dei mezzi di informazione.

Passano appena ventiquattr'ore da questi fatti ed esplode (metaforicamente) un'altra bomba: i giornali radio delle 12 e delle 13 di lunedì 2 ottobre danno notizia di un nuovo assalto telematico, che avrebbe bloccato tutti i sistemi informativi della regione Friuli-Venezia Giulia. Misteriosamente subito dopo l'informazione scompare dai notiziari. Che cosa è successo? Che il magistrato che indaga sulla Falange armata, il PM Pietro Saviotti, ha chiesto il silenzio stampa. Il giorno dopo la Repubblica si adegua e ignora la notizia proveniente da Trieste, ma ritorna sul cosiddetto assalto di due giorni prima, titolando: «Così hanno violato Bankitalia». Finalmente nell'articolo si precisa che «gli elaboratori... sono sempre rimasti nel controllo dell'Isitituto stesso, né sono penetrabili dall'esterno». E allora, perché tanto clamore? Ma

Attenzione alla password!

Nella maggior parte delle violazioni di sistemi informativi il primo colpevole è proprio l'amministratore di sistema. Se è vero che la sicurezza assoluta, al cento per cento, non è mai raggiungibile, è anche vero che si possono assumere precauzioni che consentono di ottenere la quasi inviolabilità.

I metodi sono molti, e devono essere adottati tutti insieme: in primo luogo chiudere tutti i buchi hardware e software, che nella maggior parte dei casi sono noti a quelli che lavorano sulle diverse «piattaforme», poi adottare una corretta gestione delle password e addestrare gli utenti a custodirle con attenzione. Ecco un piccolo elenco delle precauzioni che dovrebbero essere considerate obbligatorie.

1. Adottare uno schema di password che obblighi a usare segni di interpunzione e numeri, oltre che lettere, distinguendo le maiuscole dalle minuscole (vedi il sistema di MC-link). Questo aumenta enormemente il numero delle combinazioni possibili e evita le stringhe tipo «123456», «PIPPO» o «Luigi», nel caso che il titolare si chiami, appunto, Luigi. Queste password sono la gioia degli hacker.

2. Archiviare le password crittografate con un sistema «one way» (cioè a senso unico, anche questo metodo è adottato da MC-link). L'algoritmo «one way» non consente di ricostruire la password all'indietro, cioè partendo dalla stringa in codice. Chi riuscisse ad entrare nell'archivio troverebbe dati praticamente inutilizzabili.

3. Obbligare gli utenti a cambiare periodicamente la password, in genere una volta al mese. Se l'utente non cambia la password, alla scadenza gli viene negato l'accesso: deve rivolgersi all'amministratore di sistema e farsi riabilitare, dopo la somministrazione di una ramanzina. Un metodo più pratico e meno umiliante è la comparsa di un messaggio: «È l'ultima volta che entri con questa password, cambiala!».

4. Il punto precente invoglia gli utenti ad attaccare al computer un foglietto con la password. Per questo l'amministratore, o l'addetto alla sicurezza, dovrebbe girare spesso per gli uffici e verificare che non si vedano password in giro, adottando anche sanzioni contro gli imprudenti.

Tutto questo assicura un'ottima protezione contro gli accessi con password rubate, ma non protegge nulla se non c'è un preciso collegamento tra la password e il suo titolare. Concedere un abbonamento senza accertarsi, con la necessaria diligenza, dell'identità del cliente, rende impossibile l'identificazione di responsabili di atti delittuosi. Non parliamo poi di recenti azioni promozionali, con le quali sono state messe in giro centinaia di migliaia di dischetti con le stesse password: è come andarsene in vacanza per un mese lasciando spalancata la porta di casa.

altri giornali, fra i quali il Corriere della Sera e molti quotidiani locali, hanno ritenuto di dare notizia della violazione del sistema di Trieste. Che è stata un'azione anche meno dannosa di quella perpetrata ai danni del collegamento Internet della Banca d'Italia, perché hanno lasciato il solito messaggio sulle macchine dell'ufficio stampa della Regione, collegate a Internet, affermando in sostanza: «la vera Falange siamo noi e possiamo fare danni terribili, quelli di ieri sono dei dilettanti, degli abusivi». Le macchine sono state staccate per il tempo necessario alla Digos per effettuare i rilievi ed è stato messo in funzione il sistema di riserva.

Dunque, per ora, il «rischio Falange Armata» non dovrebbe essere grave come lo si vorrebbe dipingere. Fra l'altro si sta profilando l'ipotesi che il primo «attentato telematico» della misteriosa organizzazione, quello del 1. dicembre '94 all'agenzia ADN Kronos, non sia stato portato dall'esterno, ma dall'interno del sistema. E questo cambia tutte le valutazioni sull'accaduto, in particolare l'allarme giustamente creato dall'ipotesi che ci sia qualcuno in grado di penetrare senza problemi in qualsiasi rete. Se riassumiamo i fatti che fino a oggi sono stati resi noti, finora non si sarebbe verificata nessuna vera intrusione in sistemi di importanza vitale, nonostante i «terroristi digitali» affermino di possedere le chiavi di tutti i computer che governano i centri nevralgici della nostra penisola.

Questa è la situazione, fino a prova contraria, che si può ricostruire scavando fra i titoli ad effetto. Resta da considerare un particolare importante, in materia di diritto-dovere dell'informazione. È comprensibile, e probabilmente opportuno, che un magistrato che conduce un'inchiesta delicatissima cerchi di ottenere il silenzio stampa su certe notizie che possono oggettivamente «fare il gioco del nemico». Altrettanto comprensibile, e forse corretto, è che la stampa non voglia rinunciare al suo ruolo e fornisca ugualmente l'informazione. Ma c'è modo e modo: si deve trovare una via di mezzo tra l'accettazione della censura scelta dalla Repubblica e il riportare per esteso il «comunicato della Falange», come hanno fatto molti altri giornali. Una piccola notizia (anche perché è piccolo il fatto), senza citazioni testuali, soddisferebbe il dovere di cronaca e non favorirebbe la cercata diffusione di proclami inquietanti e di allarmi forse ingiustificati.

Ma le «bombe» esplodono sempre

Sulla base delle informazioni che ho riportato, la mia opinione è che queste imprese non siano da attribuire a un gruppo terroristico ben organizzato e in grado di colpire qualsiasi importante sistema informativo. Lo indica il fatto che quella che viene presentata come un'azione dimostrativa della «potenza di fuoco» della sedicente organizzazione terroristica, di fatto è l'equivalente digitale di un banale furto di polli. Se la cosiddetta Falange esiste e di-

1) Terrorismo informatico o terrorismo giornalistico? (da la Repubblica del 1 ottobre).

2) Più correttamente l'Unità si chiede: «Avvertimento o brutto scherzo?».

3) Il giorno dopo l'episodio è ridimensionato, ma la Repubblica insiste...

4) Il Gazzettino riporta in prima pagina l'attacco di Trieste, con un intelligente commento di Roberto Vacca.

5) La Tribuna di Treviso passa la notizia nelle pagine interne, senza citare il comunicato: c'è la notizia, non c'è il terrorismo giornalistico.

spone di elenchi di delicate password (che possono diventare inutili in pochi attimi, basta cambiarle!), potrebbe dimostrarlo violando realmente un importante sistema informativo, magari senza provocare gravi danni, ma facendo capire inequivocabilmente che si tratta di un attacco portato o organizzato dall'esterno del sistema colpito.

Questo significa che non credo all'esistenza dei ciberterroristi? Non ho informazioni sufficienti per esprimere una valutazione sull'esistenza «reale» di queste persone, ma sono certo della loro presenza «virtuale». Nel senso che, indipendentemente dalla loro origine, queste azioni ottengono l'effetto di atti terroristici, perché spargono il timore fra la gente. Potremmo fare l'ipotesi che tutte queste azioni (e, forse, anche altre che potrebbero non essere state comunicate ai mezzi di informazione) siano opera di individui diversi, non collegati tra loro, ciascuno dei quali avrebbe agito in totale autonomia, per puro spirito di imitazione. In

L'urgenza della legge

Il disegno di legge 1901 *bis* sulla protezione dei dati personali, in discussione al Parlamento, impone al responsabile del trattamento di adottare tutte le misure necessarie per la sicurezza dei dati, *anche in relazione alle conoscenze acquisite in base al progresso tecnico, alla natura dei dati e alle specifiche caratteristiche del trattamento, in modo da ridurre al minimo, mediate l'adozione di idonee e preventive misure di protezione, i rischi di distruzione o perdita, anche accidentale, dei dati, di accesso non autorizzato o di trattamento non consentito o non conforme alle finalità della raccolta* (art. 15).

È chiaro che per conseguire questo risultato è necessario prima di tutto provvedere

Intervista al maggiore Mauro Floriani

Le Fiamme Gialle: specialisti per passione

Mauro Floriani.

Il maggiore Mauro Floriani comanda il II Gruppo della IX Legione della Guardia di Finanza, specializzato nella repressione di traffici illeciti che vanno al di là delle normali violazioni alla normativa tributaria. In questo reparto la terza Compagnia si occupa specificamente della pirateria del software, sotto la direzione del sostituto procuratore Giuseppe Corasaniti, e ha messo a segno importanti azioni contro i duplicatori abusivi.

* * *

***M**aggiore Floriani, anche nella vostra ultima operazione in materia di duplicazione illecita di programmi avete agito senza il supporto di consulenti esterni, ottenendo tuttavia ottimi risultati. C'è quindi un settore specializzato all'interno della Guardia di Finanza?*

Non abbiamo al'interno del nostro corpo una specializzazione in questo settore. Prima di tutto perché è nuovo, e non siamo moltissimi, come tutti sanno. Il nostro gruppo di specialisti si è formato spontaneamente e cerca di stare al passo con i tempi.

Stiamo cercando di avviare i neo-finanzieri, e anche sottufficiali e ufficiali, a una conoscenza del settore informatico quanto più estesa possibile. Prima di tutto per una possibilità di utilizzo diretto, ma anche per sviluppare l'attività di polizia in questo settore, che molti elementi ci fanno pensare che potrebbe essere la criminalità del futuro.

Cerchiamo di avere una base su cui poter lavorare, ma per quanto riguarda la nostra specializzazione diciamo che è un po' affidata all'iniziativa dei singoli.

Abbiamo visto che questo è un settore nuovo, in cui si deve lavorare bene. C'è la necessità di ragazzi che vogliano fare qualche sacrificio, nel senso di rimanere un po' di più, al di là dell'orario di lavoro, di comperarsi qualche manuale, oltre quello che noi, come organizzazione dello Stato, possiamo fornire.

Scambiamo idee e esperienze con altri colleghi, ci diamo un po' tutti una mano.

Noi, come II Gruppo, stiamo cercando di costituire un gruppo di ragazzi che abbiano una competenza specifica in questo settore perché, qualora ce ne sia la necessità, possiamo utilizzare sempre gli stessi: quelli della terza Compagnia, e anche quelli della quarta, i «Baschi verdi», che hanno dei servizi anche in questa materia *(i «Baschi verdi» sono specializzati in antiterrorismo e operazioni di pronto impiego, ndr).*

***L**a pirateria del software è esclusivamente opera di piccoli operatori, o ci sono di mezzo organizzazioni importanti?*

Non ci sono delle organizzazioni o delle strutture criminali consolidate, per ora. Noi comunque cerchiamo di capire se ci sono prospettive di costituzione di organizzazioni di questo tipo. Non abbiamo elementi certi per dire che ci sono delle strutture come per il contrabbando o per la pirateria audiovisiva, per la quale ci sono collegamenti diretti con organizzazioni camorristiche, come è emerso qualche mese fa in un'importante operazione dei nostri colleghi dell'Arma dei Carabinieri e anche in una che abbiamo condotto

alla sicurezza del sistema in sé. Considerando poi che la maggior parte dei sistemi informativi contiene un archivio di dati personali (se non altro l'elenco degli abbonati, o le basi dati di clienti e fornitori nel computer di un'azienda) la norma citata obbligherà tutti i gestori ad adottare serie misure di sicurezza, in mancanza delle quali possono sorgere gravi responsabilità civili e penali. Norme ancora più precise su questa materia dovrebbero essere contenute nella legge-delega prevista dal 1901 *ter*, che dovrebbe contenere anche la definizione della non responsabilità dei gestori dei sistemi telematici in relazione a eventuali contenuti illeciti immessi da terzi, e anche stabilire i casi in cui un sistema telematico ricade nell'ambito della legislazione sulla stampa, con l'obbligo di registrazione come testata giornalistica. Si porrà così fine a una lunga (e abbastanza inutile) discussione su questi argomenti. L'approvazione dei ddl 1901 *bis* e *ter* è quindi urgente, non solo per adempiere a precisi obblighi internazionali, ma anche per mettere ordine in un settore nel quale oggi regna il caos. Un altro aspetto che fino ad ora non è stato considerato, ma che dovrebbe essere a sua volta oggetto di disposizioni specifiche, riguarda i «buchi» che sono caratteristici di alcuni sistemi, e che di solito non vengono segnalati dai produttori, anche se sono noti a tutti gli esperti. Le norme sulla sicurezza dei prodotti industriali dovrebbero bastare, ma, data la delicatezza della materia, non sarebbe eccessivo un preciso richiamo nella emananda legge-delega.

noi in Campania, sulla base di informazioni assunte a Roma. Però i vantaggi di attività illecite di questo tipo sono enormi, soprattutto se si tratta di prodotti, come stiamo vedendo recentemente, di tecnologia superiore ai primi grossolani tentivi di duplicazione, e anche perché le punizioni sono limitate e non possiamo certo pretendere pene «islamiche» per questo tipo di reati.

Ma, seguendo le precedenti esperienze del contrabbando e della pirateria audiovisiva, abbiamo motivo di ritenere che alla lunga anche in questo settore si possano verificare sviluppi preoccupanti. Prendiamo, per esempio, la pirateria telematica. Immaginiamo che qualcuno riesca a entrare nei sistemi di una banca (il che è molto difficile) e riesca ad acquisire informazioni riservate. Viene a sapere che una persona si trova in uno stato di necessità, e da qui all'usura il passaggio è diretto. Comunque ritengo che se alla lunga verranno fuori rapporti con organizzazioni criminali di livello superiore, dovrà indagare il reparto che si occupa specificamente di criminalità organizzata.

Il nostro è un lavoro locale, prevalentemente su Roma. È chiaro che se il livello si innalza, dovrà innalzarsi anche il livello della struttura che se ne occupa.

***Q**uindi il vostro lavoro è diretto soprattutto alla repressione della pirateria informatica nelle forme che oggi sono più preoccupanti.*

Certo, non perdiamo tempo con lo studentello che, a tempo perso, duplica programmi. Ma seguiamo anche questo fenomeno, cerchiamo di verificare, di fare un'attività di «intelligence», nel nostro piccolo, per capire gli sviluppi di questo tipo di attività illegali.

***U**n'ultima domanda, maggiore Floriani. Qualche difensore di persone indagate per violazioni al DL 518 ha sollevato l'obiezione che i sequestri di software copiato abusivamente non sono stati compiuti durante perquisizioni ordinate dall'autorità giudiziaria, ma nel corso di verifiche compiute dalla Guardia di Finanza di propria iniziativa, sulla base della normativa tributaria e della legge del '29...*

La legge n. 4 del 7 gennaio 1929 è una norma cardine del sistema tributario, perché permette di fare comunque controlli per perseguire violazioni in materia finanziaria e tributaria. Noi però siamo molto attenti a questo aspetto, anche in funzione delle nuove norme di procedura penale: non vale la pena forzare la mano, per vedersi poi invalidato tutto. Non si ottiene nulla, si vanifica un'attività per la quale si può attendere l'autorizzazione del magistrato.

A me, come comandante del mio reparto, non interessa fare immediatamente un sequestro per dimostrare che sono bravo, per aumentare il rendimento del reparto. Può capitare di trovare incidentalmente software irregolare, ma tendenzialmente noi dobbiamo essere in grado di avere delle informazioni precise e di operare in modo che quello che facciamo sia utile e arrivi all'ultimo grado di giudizio.

Lo potremmo fare sempre, non dico casualmente, ma quasi. Penso che potrei fare un intervento al giorno, in qualsiasi amministrazione dello Stato o in qualsiasi azienda privata, e troverei programmi duplicati. Credo che questo lo sappiano tutti...

questo caso non esisterebbe «fisicamentre» un'organizzazione di ciberterroristi. Però gli effetti sono gli stessi, esattamente come si verifica nelle applicazioni delle tecnologie della realtà virtuale: il sistema informatico ci fa credere che una cosa esiste, e invece non c'è. Terrorismo virtuale, dunque. Una situazione inquietante, di fronte alla quale non sappiamo assolutamente che fare, se non sperare che magistrati e forze dell'ordine facciano luce e identifichino i responsabili.

In conclusione, tutto questo mi fa temere che dovremo abituarci a fare i conti con una «realtà virtuale» molto meno divertente dei grossolani esperimenti che vediamo nelle fiere. L'informazioni digitalizzata, dove ogni bit è uguale a un altro, dove non c'è differenza tra il bit autentico e quello contraffatto, si presta a ogni forma di manipolazione occulta. Molti hanno visto un filmato dimostrativo di Silicon Graphics, nel quale si vede la ripresa di una vettura che corre sull'autostrada. Sembra, e forse è, un vero film, cioè una scena ripresa dal vivo con una macchina da presa. Ma in pochi secondi vediamo l'auto che cambia forma e colore, e diventa di un'altra marca, continuando a correre sul nastro d'asfalto. Chi vede solo la prima parte del filmato può giurare in totale buona fede che si tratta di un certo tipo di auto, di quel colore. Chi vede solo la seconda può affermare, con altrettanta buona fede, che si tratta di un altro modello e di un altro colore. Qual è la verità? Forse non esiste, forse tutta la sequenza è stata creata nella memoria di un computer. Nella realtà potrebbero non esistere né l'una né l'altra automobile, potrebbero non esistere nemmeno quell'autostrada e quel paesaggio. Eppure quando ho visto l'inizio di quella sequenza ero convinto che si trattasse di una vera ripresa cinematografica. Se non avessi assistito alla metamorfosi, non avrei avuto nessun dubbio: due riprese diverse, con due vetture diverse.

Il cinema si è impadronito di questa tecnologia. Un attore muore durante le riprese? Condoglianze alla signora, noi giriamo le scene che mancano «sintetizzando» il personaggio. Chi è in grado di distinguere l'attore vero da quello virtuale? Lasciamo la fiction e proviamo a immaginare la stessa applicazione in una situazione reale: un tale è accusato di un delitto, in tribunale viene fatto vedere un filmato nel quale lo si vede nell'atto di compiere il crimine. È una prova? Oggi lo è, domani potrebbe non esserlo.

Possiamo appena intuire la prospettiva di un enorme cambiamento culturale. Oggi siamo convinti che sia reale tutto quello che vediamo, tutto quello che tocchiamo con mano. Diciamo, come San Tommaso, che se vediamo, crediamo. Ma sappiamo anche quello che vedremo domani, con la stessa apparenza realistica, potrebbe essere «virtuale», cioè non esistere nella realtà: è la concezione stessa della «realtà» che viene scossa dalle fondamenta. C'è un'intera filosofia da costruire dal nulla. Come faremo?

Problemi giuridici sulle intercettazioni telefoniche

Le polemiche sorte tra i magistrati e tra questi e gli avvocati dopo la rivelazione dei contenuti delle telefonate del «latitante di Hammamet» hanno fatto passare in secondo piano alcuni aspetti molto importanti della vicenda, legati a norme di procedura penale, diritto internazionale e protezione della privacy, discusse ampiamente anche nel nostro Forum multimediale «La società dell'informazione».

La Procura di Milano non ha voluto rivelare le tecniche usate per intercettare le telefonate (in arrivo, in partenza o tutte?), limitandosi a puntualizzare il fatto che l'operazione è stata compiuta dal territorio italiano. Ma chi conosce il funzionamento delle centrali ISDN sa che l'operazione non è complessa, almeno in teoria. È complicato invece il profilo giuridico dell'operazione sul piano dei rapporti internazionali: è stata violata la sovranità di un paese straniero? Con le tecniche di intercettazione tradizionali, sulle vecchie centrali decadiche, sarebbe stato necessario un intervento «hardware» da compiere sul posto, regolato quindi da accordi tra i due Stati. Ora invece in molti casi è possibile intercettare conversazioni e flussi di dati senza dover intervenire materialmente sui fili, praticamente con le stesse tecniche degli «hackers».

Questo però ci riporta a un problema ancora irrisolto sul piano giuridico (ne ho parlato sul numero 154 di questa rivista): dove è stata commessa un'azione telematica, nella quale, per la natura stessa dell'azione, i suoi effetti si verificano in un luogo diverso da quello in cui è stata commessa? Il problemasi pone sia per gli atti illeciti, sia per quelli leciti. Per esempio, in molti casi è importante il luogo nel quale è stato stipulato un contratto; in genere, quando i contraenti si trovano in località diverse e il luogo non è stabilito convenzionalmente, il contratto si considera stipulato nel luogo in cui viene perfezionato. Ma il ciberspazio non è un «luogo» giuridicamente riconoscibile!

Sul piano sostanziale resta da fare un'ultima osservazione: se le centrali telefoniche ISDN facilitano il lavoro degli inquirenti nelle intercettazioni sulle linee di possibili autori di gravi reati, in teoria si prestano anche a facilitare le intrusioni di abili pirati telematici. Potrebbe Telecom Italia rassicurarci sul fatto che le sue centrali ISDN sono ragionevolmente a prova di «hacker»?