CARLO SARZANA

GLI ABUSI NEL SETTORE INFORMATICO. SPUNTI PER UNA RICERCA CRIMINOLOGICA E VITTIMOLOGICA

SOMMARIO 1. Premessa. — 2. Le iniziative internazionali di studio e di ricerca in tema di criminalità informatica e di vulnerabilità della società informatizzata. — 3. Brevi cenni sulla vulnerabilità dei sistemi informatizzati con p.r. al settore bancario e borsistico ed ai sistemi di votazione elettronica. — 4. Gli *hackers* all'attacco dei *computers*: il c.d. virus informatico. — 5. Spionaggio industriale e « furto di tecnologia ». — 6. Le risultanze dei *computers* e la prova del reato: casistica. — 7. Rilievi conclusivi.

1. Premessa.

Il presente articolo si occupa dei comportamenti illeciti nel settore dell'informatica da un punto di vista prevalentemente criminologico e vittimologico ed in relazione a comportamenti non soltanto dolosi ma anche colposi: per questa ragione si è preferito usare il termine assai comprensivo di « abusi » piuttosto che quello di « delitti ». L'articolo intende anche esaminare alcuni particolari aspetti della c.d. vulnerabilità della società informatizzata, citando episodi particolarmente significativi avvenuti nel settore finanziario e bancario, ed enunciando alcuni problemi sorti nell'ambito dei sistemi elettronici di votazione, sottolineando, in conclusione, la necessità di una attenta considerazione dei pericoli insiti in comportamenti fondati sulla cieca fiducia nell'affidabilità delle operazioni del *computer*. Altro argomento che sarà esaminato sarà quello relativo all'attività degli *hackers* e, con particolare riguardo, al sabotaggio dei *computers* attuato mediante l'introduzione in essi del c.d. virus informatico. Infine l'articolo si occuperà dello spionaggio informatico e dei suoi riflessi internazionali e, più in particolare, del c.d. furto di tecnologia che viene praticato ai danni principalmente di imprese *leaders*

* Il testo che segue riproduce, con modifiche ed ampliamenti, la relazione presentata dall'autore al 4° Congresso Internazionale sul tema « Informatica e regolamentazioni giuridiche », organizzato dal CED della Cassazione a Roma dal 16 al 21 maggio 1988.

nel campo dell'informatica ed i cui aspetti politici e giuridici meriterebbero — sia detto per inciso — di essere ulteriormente approfonditi.

L'opportunità di creare un osservatorio permanente sul fenomeno della criminalità informatica al fine di acquisire dati specifici, continui ed affidabili sull'andamento del fenomeno stesso è infine sostenuta nei rilievi conclusivi.

2. Le iniziative internazionali di studio e di ricerca in tema di criminalità informatica e di vulnerabilità della società informatizzata.

L'interesse di alcuni governi nei riguardi dei fenomeni sopra indicati risale alla seconda metà degli anni '70 allorché il governo svedese istituì il Comitato sulla vulnerabilità della società informatizzata, seguito poi in questa iniziativa da altri paesi scandinavi (Norvegia).

Nei Paesi Bassi recentissimamente il « Dutch General Accounting Offices » ha elaborato per il Parlamento un documento nel quale afferma che i sistemi informatizzati governativi sono « molto vulnerabili » e mettono in pericolo gli interessi della società (vedi TDR, febbraio 1989): si sollecita quindi l'intervento del Ministro dell'Interno che è responsabile del coordinamento. Lo stesso Ministro, tuttavia, in un recente Libro Bianco sui sistemi pubblici di informazione, ha esplicitamente ammesso la situazione di vulnerabilità dei sistemi in questione, considerata come uno degli effetti negativi della crescente dipendenza del governo dai sistemi informatici.

Dal canto loro, le grandi organizzazioni internazionali cominciarono ad esaminare ed a studiare i fenomeni in questione all'inizio degli anni '80. L'OCSE, dopo aver organizzato nel 1981 a Sigüenza (Spagna) un importante seminario sulle vulnerabilità della società informatizzata, creò nel 1984 un gruppo di esperti per studiare gli aspetti giuridici e socio-criminologici della frode informatica. Nel 1985 in seno al Comitato per i problemi criminali del Consiglio d'Europa venne creato un Comitato ristretto di esperti, il cui lavoro è terminato nel marzo scorso, con l'incarico di studiare il fenomeno della criminalità informatica e di preparare anche delle *guidelines* da sottoporre ai Paesi Membri per la redazione o l'armonizzazione delle leggi nazionali dirette a reprimere la particolare criminalità. Infine è da dire che la Commissione della Comunità Europea ha iniziato sin dal 1982 ad interessarsi del problema della vulnerabilità della società informatizzata in Europa, patrocinando due importanti ricerche.

La prima di esse, iniziata appunto nel 1982 e terminata nel 1983 e diretta dall'esperto francese Jean Chamoux coadiuvato da una ristretta equipe di ricercatori, riguardava la situazione in cinque Paesi

europei (Belgio, Francia, Italia, Regno Unito e Repubblica Federale di Germania). La ricerca ha esaminato ben 115 casi di abusi informatici e di incidenti nel settore in questione, ed ha concluso formulando una serie di raccomandazioni ed uno schema di azione a livello comunitario. L'idea di fondo della ricerca in questione era che la crescente informatizzazione dei servizi economici e sociali e la loro crescente interconnessione, mentre aveva avuto come effetto vantaggi notevoli nel campo della circolazione delle informazioni, aveva creato d'altro canto rischi gravi di incidenti e di frodi. I ricercatori hanno sottolineato che l'accesso non autorizzato alle banche di dati o agli schedari di una società può arrecare ai soggetti interessati danni economici anche di rilevante entità: ed infatti gli incidenti verificatisi e gli abusi posti in essere costavano già alla Comunità milioni di ECU annualmente.

La seconda ricerca aveva come oggetto la vulnerabilità dei sistemi informatici ed i suoi effetti intersettoriali, economici e sociali, ed è stata coordinata dall'ente italiano ISTEV (Istituto per lo Studio della Vulnerabilità delle Società Tecnologicamente Evolute) diretto dal Prof. Bisogni. L'idea guida della ricerca, i cui risultati finali sono stati presentati nel convegno organizzato dall'ISTEV a Roma nell'aprile scorso, era quella riguardante l'identificazione del ruolo dei sistemi di *computers* usati come supporto nelle attività di produzione di beni e servizi: si intendeva quindi analizzare gli effetti derivanti dall'accesso illegittimo a tali sistemi o dal loro cattivo funzionamento sia in termini economici che sociali. L'importanza e la dimensione sociale degli incidenti e delle *defaillances* e la sollecitazione dei pubblici poteri a darsi carico delle conseguenze derivate dai predetti incidenti sono stati, in un certo senso, un *leit-motif* della ricerca in questione.

La Commissione ha dato inoltre il via, con la collaborazione finanziaria di vari *sponsors*, ad altre ricerche nel campo della sicurezza dei sistemi informatici. Una di queste, affidata alla società Coopers and Lybrand, ha avuto come tema quello relativo alla sicurezza delle reti ed alle raccomandazioni minime per gli utenti ed i costruttori di sistemi informatici. La ricerca in questione ha coinvolto venti grandi organizzazioni nell'ambito dei Paesi della CEE, tra cui tre enti italiani (la BNL, la Rizzoli Editore, la Telettra). Secondo i primi risultati, peraltro soltanto una delle venti aziende sarebbe in possesso di un sistema informatico sufficientemente sicuro. La ricerca si è conclusa con una serie di raccomandazioni dirette ad implementare i sistemi di protezione delle reti ed a sensibilizzare gli utenti, i venditori e le autorità pubbliche al problema della sicurezza.

L'argomento della criminalità informatica in particolare è stato esaminato nel corso di una recente riunione svoltasi nel maggio 1988 in seno all'Osservatorio Giuridico della Commissione, un gruppo consultivo informale costituito sin dal 1985 e che si occupa dell'impatto delle nuove tecnologie dell'informazione sul settore legislativo. In tale riunione è stato affermato, fra l'altro, che la Commissione

avrebbe dovuto promuovere in tutti i Paesi membri della CEE l'applicazione dei principi direttivi per i legislatori nazionali in corso di elaborazione da parte del Comitato ristretto di esperti per lo studio della criminalità informatica creato in seno al Consiglio d'Europa.

Da ultimo, il Segretario del Comitato per la Politica dell'Informatica, dell'Informazione e delle Comunicazioni, istituito in seno all'OCSE, accogliendo le idee espresse in più sedi dalla delegazione italiana, ha proposto al Comitato di svolgere una ricerca relativa alla sicurezza delle reti informatiche e di telecomunicazioni. La ricerca si svolgerà in due fasi, secondo il progetto: in una fase preliminare saranno definite con precisione le questioni legate alla sicurezza dei sistemi mentre nella seconda fase si effettuerà un esame approfondito delle misure tecniche esistenti ed in preparazione, dei metodi di gestione (ivi compresi l'*auditing* informatico, l'assicurazione e la gestione dei rischi, le misure di *recovery*, ecc.) ed, infine, delle misure adottate dai vari Governi nel campo civile, penale ed amministrativo.

Il rapporto finale dovrebbe offrire una base documentale suscettibile di dar luogo alla formazione di apposite politiche.

Anche la Camera di Commercio Internazionale ha pubblicato nel luglio del 1988 un rapporto dal titolo « Computer Related Crime and Criminal Law: an International Business Wiew » le cui conclusioni possono così riassumersi: *a*) esistono diverse attività criminali fondate sull'accesso o l'utilizzazione *non autorizzati* degli elaboratori e ciò costituisce una seria minaccia per i sistemi telematici; *b*) i proprietari e gli utilizzatori di questi sistemi, e cioè dei sistemi informatizzati di telecomunicazione e di informazione, hanno necessità di ottenere dal diritto penale un aiuto efficace in materia di protezione dei loro patrimoni, sovente preziosi, di informazioni; *c*) le leggi esistenti, a meno che non siano specificamente redatte in funzione di delitti associati all'informatica, possono non applicarsi oppure non possono essere adattate al nuovo fenomeno. Anche quando le leggi esistenti possono essere applicate, le sanzioni penali sono in genere insufficienti; *d*) l'*iter* procedimentale non è sempre assicurato in maniera efficace anche a livello nazionale ed il carattere internazionale di molti dei delitti associati all'informatica aggrava il problema. A seguito di tali conclusioni la CCI ha ritenuto opportuno rivolgere diverse raccomandazioni alla Comunità Economica affinché solleciti gli organi legislativi nazionali a vegliare affinché: *a*) tutte le maggiori minacce siano correttamente considerate nel diritto penale nazionale; *b*) l'istruzione e le procedure relative ai delitti associati all'informatica siano efficacemente assicurate a livello nazionale; *c*) i governi nazionali e le organizzazioni internazionali coordino le legislazioni relative ai delitti associati all'informatica e facciano in modo che la criminalità al di là delle frontiere possa essere, e sia, effettivamente perseguita.

3. Brevi cenni sulla vulnerabilità dei sistemi informatizzati con particolare riguardo al settore bancario e borsistico ed ai sistemi di votazione elettronica.

I sistemi informatizzati appaiono vulnerabili non soltanto nei confronti di atti intenzionali ma anche in relazione a semplici atti di negligenza e perfino ad atti non riconducibili al dolo o alla colpa di un individuo. Gli errori conseguenti ad inesatto *data entry* o ad una compilazione del *software* non accurata possono produrre in determinate circostanze gravi conseguenze ad individui ed a collettività. Gli esperti affermano in modo concorde che in generale i sistemi contengono uno o più errori, e spesso un cumulo di errori, che vengono alla luce soltanto per caso e che comunque sono spesso molto difficili da correggere. Il discorso diviene più difficile allorché si tratta dei sistemi esperti, come già accennato da me in altra sede (vedi la relazione dal titolo *Tecnologia informatica e criminalità. Aspetti nazionali ed internazionali*, in *Quaderni della Giustizia*, n. 64 del 1986, p. 76).

Come è noto i sistemi esperti, vanno sviluppandosi sempre più ed in alcuni settori, come quello medico e legale, vengono oggi usati abbastanza frequentemente come ausilio alla diagnosi e cura nel settore delle infezioni batteriche, della medicina interna e del glaucoma. Sperimentazioni importanti vengono condotte nel settore psicologico, ingegneristico, del trasporto aereo, nucleare, industriale, ecc.

Appare molto difficile individuare le singole responsabilità, specie dal punto di vista penalistico, nel caso in cui il cattivo funzionamento di un sistema esperto abbia cagionato danni fisici o economici giacché, com'è noto, gli errori possono derivare separatamente o congiuntamente, dalla condotta dei programmatori, degli esperti che hanno creato la base di conoscenza, dei distributori, dei produttori, ed in alcuni casi, anche degli utilizzatori di tali sistemi[1].

Nel caso particolare di un sistema esperto adoperato per il controllo del traffico aereo, l'autore che si è occupato dell'argomento, Tod M. Turley (in *Computer Law Journal*, vol. VIII, n. 5, 1988, p. 455) ha affermato che i danni da esso eventualmente cagionati possono farsi risalire ad una combinazione di 4 fonti di errore e cioè: *a*) errori nel programma (logici o di redazione); *b*) errori nella base di conoscenza; *c*) errori dovuti alla incompetenza nell'uso del programma o ad una fiducia non appropriata in esso risposta; *d*) insufficienze dell'*hardware*.

[1] In tema di responsabilità nell'uso dei sistemi esperti, vedi da ultimo per la dottrina statunitense, M. Gemignani, *Potential Liability for Use of Expert Systems*, in *Idea*, vol. 29, n. 2. Per la dottrina italiana, vedi G. Corrias Lucente, *Prime considerazioni in tema di responsabilità penale e gestione di sistemi informatizzati con particolare riguardo ai sistemi esperti*, in questa *Rivista*, 1989, p. 117 ss.

In particolare, va ricordato che siccome anche in questo settore i sistemi esperti sono creati dallo sforzo congiunto di programmatori ed esperti in un determinato settore, appare estremamente difficile individuare le particolari responsabilità in caso di irregolare funzionamento del sistema stesso in un ambiente quale, ad es., quello del traffico aereo che può definirsi senz'altro ad alto rischio.

Passando ora ad altro argomento, è opportuno ricordare che anche la c.d. « mistica » del *computer* dalla quale deriva una esagerata fiducia nelle risultanze dei processi informatizzati, ha favorito e favorisce in molti casi la commissione di crimini che, in sistemi manuali, sarebbero stati probabilmente impediti. Nel citato rapporto redatto nel 1984 per conto della Commissione CEE dall'« equipe » diretta dall'esperto francese Jean Chamoux, vi è un episodio molto significativo riguardante il cambiamento di mentalità di un cassiere di banca nei confronti di sistemi automatizzati e concretatosi nell'accettare come verità assoluta i dati forniti dal terminale. Il caso è avvenuto in Belgio ed è descritto nel rapporto di cui sopra. Un individuo aveva depositato in banca un assegno falso di 76 milioni di FB avvisando i funzionari che avrebbe potuto ritirare poco dopo una parte della somma: ciò al fine di trovare disponibilità di fondi. Allorché il soggetto si era presentato per l'incasso, il cassiere aveva interrogato l'elaboratore il quale aveva confermato che esisteva la disponibilità della somma in concreto richiesta (si trattava soltanto di 73 milioni...!). In realtà vi era un piccolo errore nel sistema informatico della Banca: esso *non* indicava in questi casi al cassiere la dizione « *salvo buon fine* » e questo piccolo errore aveva permesso la commissione del crimine. Probabilmente in un sistema di gestione manuale la circostanza non sarebbe sfuggita.

I pericoli sembrano abbastanza concreti anche nell'ambito del mercato finanziario e bancario. Vi sono stati negli anni scorsi esempi notevoli dei danni che possono produrre errori o « pannes » di un sistema bancario...

Appare opportuno elencare alcuni incidenti dei quali la stampa ha dato notizia. Il primo episodio si è verificato alla fine del novembre 1985 (vedi *Computerworld* del 2 dicembre 1985) ed ha interessato una grande banca di New York, broker di titoli di Stato la quale ha subito un guasto al suo sistema informatico durato un giorno e mezzo e causato — sembra — da un sovraccarico di lavoro che aveva fatto andare « in tilt » il *software*. La banca aveva continuato a ricevere dai venditori i certificati del tesoro e le obbligazioni ma si era trovata nella impossibilità — a causa della « panne » — di poterli consegnare agli acquirenti. Poiché secondo la pratica corrente nel mercato dei titoli governativi, la banca che riceve tali titoli è responsabile nei confronti dei venditori per il pagamento dal momento della ricezione dei titoli stessi mentre gli acquirenti diventano debitori dal momento della consegna agli stessi dei titoli, la banca fu costretta a richiedere in prestito al *discount window* della Federal Reserve Bank, e al tasso di interesse del 7,5%, una somma che si aggirava tra i 20 ed i 22 miliar-

di di dollari. L'incidente causa alla Banca una perdita netta complessiva di 4-5 milioni di dollari.

La stampa ha dato poi notizia di un altro grave incidente verificatosi alla fine di settembre del 1987. Per 24 ore il Centro Informatico della Federal Reserve Bank, la Banca Centrale USA, si bloccò rendendo impossibili le grandi transazioni interbancarie e facendo salire dal 7% circa al 30% il tasso d'interesse per operazioni della durata un giorno. Per ventiquattro ore fu l'inferno secondo le ammissioni degli stessi funzionari della Federale Reserve. Le più grandi banche mondiali rimasero senza liquidità per un giorno intero e gli operatori dovettero cercare altrove il denaro, ingaggiando una vera caccia disperata al denaro e pagando interessi a volte elevatissimi (vedi La Stampa del 2 ottobre 1987).

Il noto esperto di fama internazionale, l'inglese Adrian Normann, ha pubblicato un articolo molto interessante in TDR dell'aprile 1987 sostenendo che, data la computerizzazione della Borsa e dei sistemi finanziari ed i sistemi di vendita e di acquisto automaticamente programmati, i disastri nei mercati finanziari possono essere causati da un *positive feedbak* che potrebbe divenire rapidamente un « nodo scorsoio » ed ha citato in proposito l'incidente verificatosi in USA il 23 gennaio 1987. Come è noto in tale giorno il Dow Jones Industrial Average, un indice composto di 30 *stocks*, salì di 64 punti e perse subito dopo 114 punti: tutto ciò nell'arco di soli settanta minuti. Il 19 ottobre 1987, conosciuto anche come il « Black Monday », il DJIA cadde di ben 508 punti, corrispondenti ad una perdita media del 22%. Questa « volatilità » del mercato è stata attribuita all'uso dei sistemi automatizzati di acquisto e vendita di titoli ed azioni, ed in particolare, all'uso di uno speciale programma chiamato *program trading*. J. Phelan, presidente del New York Stock Exchange, ha sostenuto che i *programs trading* erano, almeno parzialmente, responsabili del crollo del 19 ottobre, essendosi verificato un grande movimento contemporaneo di valuta, ed il giorno successivo, e cioè il 20 ottobre 1987, ha sospeso l'uso dei sistemi automatizzati di acquisto e vendita nella Borsa di N.Y. In seguito le più importanti organizzazioni hanno limitato grandemente o addirittura eliminato l'uso dei *programs-trading*. I critici hanno affermato tuttavia che l'eliminazione dei sistemi automatizzati nel settore del mercato finanziario produrrebbe... *the return to the Stone Age*. Credo che si possa concludere affermando che la vulnerabilità dei sistemi computerizzati, anche in questo vitale settore della vita economica di un Paese, sembra sia abbondantemente dimostrata.

La fiducia cieca nella validità dei sistemi computerizzati e cioè nella assoluta precisione ed affidabilità dei risultati di una elaborazione elettronica di dati è probabilmente alla base di grossi equivoci nel settore relativo ai sistemi elettronici di votazione.

In Italia nella passata legislatura, ed a seguito della scoperta di vari brogli elettorali, vennero presentati ben 8 progetti di legge di-

retti ad introdurre lo scrutinio elettronico nelle operazioni elettorali. Tutti i proponenti dei progetti partivano dalla premessa secondo la quale i sistemi elettronici garantivano la massima certezza nell'identificazione dei candidati eletti « sottraendoli — cito testualmente le parole della relazione che accompagnava il progetto n. 3392 del 15 gennaio 1986 — a possibili tentativi di brogli o a manomissioni elettorali ». Nell'attuale legislatura gli On.li Stegagnini e Ciccardini hanno presentato alla Camera il 28 luglio 1987 la proposta di legge n. 1256 relativa al nuovo sistema di votazione e di scrutinio per le elezioni politiche ed amministrative.

Più di recente uno dei partiti della coalizione di governo, prendendo spunto dai brogli elettorali verificatisi nella circoscrizione Napoli-Caserta è partito, lancia in resta, come afferma il quotidiano « Il Giornale Nuovo » del 27 febbraio 1988, in favore dell'introduzione del voto elettronico in quanto « esso servirebbe in modo importante alla credibilità delle istituzioni... »;

Il costo per l'introduzione delle innovazioni si aggirerebbe tra i 700 ed i 900 miliardi di lire: si dice che al Ministero dell'Interno gli esperti siano già al lavoro (vedi al riguardo l'articolo di Taviani sul « Il Giornale Nuovo » del 27 febbraio 1988). Un ricercatore del Censis, Valerio Bellini, ha esposto i risultati di una recente indagine del Censis effettuata per conto della Sweda-Enidata e pubblicata nel marzo 1987 relativa alla « permeabilità sociale all'introduzione del voto elettronico » dai quali emerge che l'atteggiamento delle persone verso questo tipo di modernizzazione è generalmente positivo: una percentuale vicina al 60% degli intervistati si è dichiarata infatti favorevole al voto elettronico che dovrebbe però essere preceduto — cito le parole di Bellini — da una intensiva campagna di informazione e sensibilizzazione dell'elettorato. Scendendo in dettaglio si vede però che il 50,3% circa degli intervistati ha espresso *dei dubbi in ordine alla regolarità del voto in tal modo espresso*, dimostrando così una notevole informazione circa la possibilità di frodi informatiche[2].

Va comunque rilevato che nonostante le opinioni espresse dai politici, la realtà non è idilliaca...

Negli Stati Uniti, infatti, dove il sistema elettronico di votazione è in uso da tempo (circa il 60% delle votazioni si svolge con questo sistema) sono state ripetutamente denunziati brogli e manomissioni dei dati e dei risultati.

La società leader del settore è stata, a quanto sembra, perseguita ben quattro volte negli ultimi sei anni per asserite frodi, quantunque

[2] Secondo un autore che si è occupato « en passant » della questione (R. Pagano), la configurazione finale del sistema di votazione elettronica che viene proposto dovrebbe consistere in postazioni elettroniche (ad es. microcomputer e lettore di schede) in tutte le sezioni elettorali e nel collegamento delle stesse ad un *computer* centrale o a *computers* circoscrizionali.

sino a questo momento non vi siano state decisioni di carattere penale.

Il più antico, ed apparentemente più documentato episodio di asserita frode nelle votazioni, si è verificato nel Texas nel 1985 in un caso nel quale un candidato alle elezioni comunali si era visto eliminare per uno scarto di soli 472 voti. Dopo 18 mesi di indagini, di esami accurati dei risultati elettorali e di interviste con gli elettori, il *manager* del candidato raccolse sufficienti elementi in ordine alla sussistenza di una frode potenziale (esistevano ben 30 elementi contraddittori) tanto che il Ministero della Giustizia decise di aprire una inchiesta[3]. A parte le frodi, vi è poi il rischio di errori[4]. A prima vista il lavoro di conteggio dei voti sembra uno dei classici compiti che il *computer* può svolgere perfettamente ... in realtà si tratta di un lavoro molto complesso, specialmente per quanto riguarda i voti di preferenza, in quanto si richiede un *software* altamente preciso ed immune in modo assoluto di errori.

La stessa società citata sopra ha ammesso esplicitamente la potenziale possibilità, ovvia del resto e notissima agli esperti, di manomissione del sistema affermando che era economicamente e tecnicamente impossibile costruire un sistema a prova di truffe o manomissioni. Uno dei più autorevoli esperti statunitensi che si è occupato recentemente della questione, Lance Hoffman, docente della prestigiosa George Washington University, Dipartimento d'ingegneria e di scienza informatica, in una ricerca eseguita per conto dell'Università con il sostegno finanziario della Markle Foundation ha affermato conclusivamente che i sistemi di votazione computerizzata *non sono così sicuri ed affidabili come dovrebbero essere*: più precisamente che le votazioni in USA sono più esposte al rischio delle frodi ed agli errori di quanto sarebbe stato normale aspettarsi. Ciò anche a causa della negligenza delle autorità nell'adottare adeguate apparecchiature e procedure per la sicurezza e l'affidabilità dei sistemi computerizzati.

Altra ricerca è stata commissionata dal « Election Watch », un progetto del Urban Policy Research Institute della California, ad un

[3] Secondo gli avversari politici del nuovo Presidente del Messico, vi sarebbe stata una colossale frode elettorale, attuata manomettendo l'elaboratore centrale in occasione delle recenti elezioni presidenziali (*Expertises des systemes d'information*, n. 109, ott. 1988).

[4] Il mensile specializzato *Expertises* sopracitato ha dato di recente notizia (n. 107 del luglio 1988) di un grave errore intervenuto nelle elezioni locali. Luis Perrier, senatore e sindaco di Val d'Oise, ha visto diminuire i suoi voti del 21% circa giacché l'elaboratore della Prefettura aveva confuso la città ed il Cantone aventi lo stesso nome, « inventando » 7.500 elettori iscritti e 4.000 votanti fittizi.

gruppo di esperti nel campo dei sistemi di votazione elettronica. Nel rapporto dal titolo « Ensuring the Integrity of Electronic Elections » redatto nel novembre 1988 da H.J. Strauss e J.R. Edwards sono descritte le possibili minacce alla integrità dei sistemi ed alla genuinità dei risultati elettorali ed indicati i metodi per prevenire i pericoli.

4. Gli *hackers* all'attacco dei *computers*. Il c.d. virus informatico.

Negli ultimi anni un nuovo tipo di criminalità informatica è apparso sulla ribalta nazionale ed internazionale: quella degli *hackers*.

Si tratta di giovani, spesso studenti, in possesso di conoscenze sorprendenti nel settore dell'informatica e della telematica, interessati, a volte in modo maniacale, allo studio dei sistemi ed alle possibilità di penetrare in essi, eludendo tutte le difese approntate dagli esperti[5].

[5] Ritengo che per comprendere con sufficiente chiarezza il c.d. *hacking* bisogna ricorrere allo studio del comportamento e quindi della psicologia degli *hackers*. Esiste una ideologia fondata sulla « separatezza » degli *hackers* rispetto alla società, « separatezza » che deriva, mi sembra, da un forte orgoglio intellettuale e che conduce ad una ipervalutazione del proprio io. Io un certo senso la sfida rivolta dagli *hackers* alla « società dell'informazione » è basata sul noto slogan secondo cui « l'informazione è potere ». Il massimo potere è quindi, in qualche modo, sinonimo di massima conoscenza.

Il comportamento degli *hackers* potrebbe essere ritenuto, tuttavia (socialmente almeno) accettabile qualora l'*hacker* ponesse la sua abilità al servizio della società, non soltanto astenendosi dal danneggiare in qualsiasi modo i sistemi ed i dati e dal servirsi delle informazioni carpite, ma anche *rivelando agli interessati*, con tempestività e precisione, le lacune riscontrate nei sistemi e consentendo loro di porvi rimedio. A proposito dell'*hacking* devo dire che in seno al Comitato ristretto di esperti del Consiglio d'Europa per lo studio della criminalità informatica, del quale sono stato il vicepresidente, ho sostenuto — ai fini della punibilità dell'accesso illegittimo ai sistemi informatici — la nuova nozione di « domicilio informatico ». Se si accetta questo concetto, allora qualsiasi ingresso abusivo, indipendentemente dallo scopo e dalle conseguenze, diviene illecito e quindi punibile. Tuttavia non può penalizzarsi indiscriminatamente l'accesso; deve esistere una condizione di punibilità e cioè il sistema « penetrato » deve essere protetto da misure di sicurezza logica: non si può penalizzare infatti chi entra in una casa le cui porte sono spalancate a tutti ed anzi vi è addirittura un cartello d'invito!

Questa condizione non è stata accettata dal legislatore francese allorché ha modificato, con la legge del gennaio 1988, il codice penale per punire l'accesso illegittimo ai sistemi informatici: questo creerà molte difficoltà all'interprete giacché occorrerà procedere ad accertamenti, non facili nei singoli casi, e d'altro canto, l'assenza di una siffatta condizione non stimolerà i produttori di *hardware* e *software* e gli stessi utenti ad occuparsi dei problemi della sicurezza.

Gli attacchi compiuti dagli *hackers* nei confronti di banche dati, anche di interesse scientifico, economico e militare non si contano letteralmente più in tutti i paesi dell'occidente. Una delle ultime imprese clamorose è stata compiuta da *hackers* della Germania Federale, appartenenti alcuni al c.d. Chaos Computer Club di Amburgo, i quali sarebbero riusciti a penetrare nello SPAN (Space Physics Analysis Network), una rete mondiale di *computers* creata dalla NASA per collegare centinaia di centri di ricerche scientifiche in tutto il mondo (in particolare nel Regno Unito, nel Canada, in Francia, in Giappone, nella stessa Germania, in Svizzera, ecc.). Questo episodio ha poi dato luogo ad una delicata vicenda internazionale in quanto, in occasione della Conferenza Securicom indetta a Parigi nella primavera del 1987, uno degli *hackers* tedeschi, il ventiseienne Steffen Wernery, coinvolto nella vicenda SPAN che aveva interessato anche dei centri informatici francesi gestiti dalla Philips French Computers System, era stato invitato dagli organizzatori del Securicom ad un dibattito relativo all'*hacking*. Il giovane era stato a suo tempo accusato ed inquisito nel suo Paese ma poi prosciolto da ogni imputazione. Appena giunto a Parigi, il 14 marzo del 1988, tuttavia venne fermato dalla Brigata finanziaria sotto l'imputazione di aver sottratto, distrutto e danneggiato volontariamente i dati gestiti dalla Società di cui sopra in almeno 10 occasioni (vedi, *Computer Fraud and Security Bullettin*, aprile 1988)[6].

Al momento attuale sono pochissimi i Paesi (USA, Canada, Francia, Svezia, Danimarca) nei quali esistono regole giuridiche che possano essere usate efficacemente per reprimere il comportamento degli *hackers* allorché questo consista nell'accesso illegittimo puro e semplice ai *network* informatici, superando i sistemi di sicurezza esistenti[7].

[6] In una relazione redatta alcuni anni fa, esprimevo il timore che l'abilità degli *hackers* potesse essere strumentalizzata a fini di spionaggio o di sabotaggio (vedi l'articolo citato al pr. 3) da parte di determinati Paesi.

Di recente la stampa, specializzata e non, ha dato notizia della scoperta nella Germania Federale ai primi di marzo di quest'anno ed a seguito di investigazioni partite da una segnalazione di uno studioso di astrofisica americano, C. Stoll, del Lawrence Berkeley Institute, della complicità di un gruppo di *hackers* tedeschi in un'attività di spionaggio informatico compiuto del KGB a partire dal 1985, relativa alla penetrazione in importanti reti e sistemi pubblici e privati in tutto il mondo concernenti le ricerche ed il programma di difesa spaziale.

La Procura della Repubblica di Karlsrue avrebbe aperto un procedimento penale nei confronti di otto *hackers* di Hannover (Lamy — Droit de l'informatique — Cahiers B/1989).

Il Ministro Federale della Giustizia ha poi dichiarato che il danno indirettamente arrecato dal gruppo di spie era enorme e superava il milione di marchi giacché, tra l'altro, occorreva cambiare radicalmente numerosissime procedure d'accesso alle reti ed ai sistemi informatici.

[7] La comprensione della potenziale pericolosità delle attività degli *hackers* sta cominciando a farsi strada anche nell'ambito giudiziario statunitense. Nel gennaio di quest'anno un *district-judge* di Los Angeles ha condannato un *hacker* di 25 anni, che era penetrato in sistemi relativi alla sicurezza nazionale, alla detenzione senza benefici di legge, ritenendo che la sua abilità costituiva un rischio per la società.

Uno degli strumenti adoperati da alcuni *hackers* dediti al vandalismo è il c.d. programma-virus, un breve programma che introdotto nel sistema « infetta » tutti gli altri programmi esistenti nel sistema stesso mediante l'inclusione di una sua copia, sino a giungere in alcuni casi al blocco totale del sistema ed a volte addirittura alla distruzione dei dati[8]. Il « virus » è particolarmente usato nei riguardi dei sistemi di *personal computers* generalmente sforniti di mezzi di protezione e nei quali gli utenti introducono spesso programmi forniti ad arte gratuitamente ma la cui provenienza non è chiara. Si sta cercando di creare programmi « vaccini » o programmi *killers* che, individuato il « virus », lo « inseguono » per eliminarlo ma la situazione non è ancora ben definita (vedi ad esempio l'articolo di Tardieu dal titolo « Un médécin sur la piste du vaccin informatique », in Liberation del 28 aprile 1988).

Anche in Italia un « virus », chiamato « Ping Pong » giacché fa comparire sul display una pallina saltellante, ha fatto la sua comparsa: la sua presenza è stata segnalata specialmente nelle Università e particolarmente al Politecnico di Torino (vedi, tra gli altri, l'articolo di C. MANCINI, in *Il Giornale* dell'8 aprile 1988). La possibilità dell'introduzione di « virus » nei sistemi pubblici ha allarmato perfino la Presidenza del Consiglio dei Ministri la quale ha diramato di recente a tutti i Ministeri una apposita circolare contenente precise raccomandazioni[9].

[8] Esistono in realtà molti tipi di « virus », alcuni « benigni » ed altri « maligni »: se ne sono scoperti sino ad oggi oltre trenta. I più noti hanno nomi pittoreschi quali il « Brain Virus » detto anche « Pakistani » dal suo luogo di origine, l'« Hebrew Virus » scoperto in Israele, il « Creeper Virus », il « IBM-X Mas Tree » apparso nella forma di albero di Natale stilizzato nel dicembre del 1987 ad opera di uno studente tedesco, l'Internet Virus lanciato in USA dal « famoso » studente della Cornell University, R. Morris, e che ha creato problemi seri a più di 6.000 *computers* della rete Arpanet e Milnet che collega centri di ricerca civili e militari in tutto il mondo, il « Marijuana Virus », il Vienna Virus, ecc. Secondo il maggior esperto del settore, lo statunitense Fred Cohen, oltre 100 mila sistemi sarebbero già stati danneggiati dai « virus ».

Di recente negli Stati Uniti, a livello federale e statale, sono stati presentati appositi disegni di legge per penalizzare specificamente questo tipo di attività illecita. Il primo, cioè quello a livello federale, dal titolo « Computer Virus Eradication Act 1989 », è stato presentato alla HR all'inizio di quest'anno e prevede pene anche detentive sino a 10 anni o a 20 anni nel caso di recidiva. Nell'aprile di quest'anno poi la Minnesota House ha approvato all'unanimità un progetto di legge che prevede una pena detentiva sino a 10 anni ed una multa sino a 50.000 dollari qualora il virus abbia prodotto danni al sistema di valore superiore a 2.500 dollari (v. *Computer Security Digest* dell'8 maggio 1989).

Di recente si è avuta notizia della prima condanna pronunciata da un Tribunale americano in tema di introduzione di virus. Il 21 ottobre dello scorso anno infatti certo D.E. Burleson, un programmatore di 40 anni, è stato condannato dal Tribunale di Fort Worth — Texas — a sette anni di detenzione per aver introdotto un virus nell'elaboratore della società di assicurazioni che lo aveva licenziato, distruggendo in tal modo ben 168 mila records. L'imputazione era di violazione di domicilio, illegale accesso ad un *computer* e danneggiamento dello stesso (v. *Expertises*, n. 111 del 9 novembre 1988 e *Corporate Security Digest* del 19 settembre 1988).

[9] Secondo il settimanale americano Times, la NSA e la CIA avrebbero sperimenta-

5. Lo spionaggio industriale ed il « furto di tecnologia ».

È noto che da tempo i prodotti di alta tecnologia (apparecchiature elettroniche, laser e fibre ottiche, elaboratori, *chips* e *software*, ecc.) sono oggetto di un'opera intensa di acquisizione illegale e di un vero e proprio mercato nero che si svolgono sia a livello nazionale che internazionale. Non è un mistero che il c.d. furto di alta tecnologia è diventato un grosso affare condotto da vere e proprie organizzazioni criminali e spesso anche da agenti di paesi stranieri.

Nell'ambito della contrapposizione Est-Ovest le aree di massima priorità sono quelle dedicate all'elettronica ed all'informatica. Gli agenti dei Paesi del blocco dell'Est hanno dedicato particolare attenzione alle società ed ai centri universitari di ricerca che, nei vari paesi della Nato, lavorano per conto della difesa, cercando di acquisire in tutti i modi dati ed informazioni sulle nuove tecnologie.

Per quanto riguarda in particolare l'URSS, le due organizzazioni più attive sono il dipartimento T del KGB ed il dipartimento B del GRU, l'agenzia di spionaggio militare dell'Armata Rossa.

Dalla parte degli S.U. la lotta viene condotta, oltre che dai Servizi Segreti, dal Department of Commerce ed, in particolare, dall'United States Customs Service che, nell'ambito di un'operazione denominata « operazione Exodus », ha cercato e cerca in tutti i modi di intercettare le esportazioni illegali di tecnologia verso i Paesi del blocco sovietico o comunque alleati dell'URSS.

Una serie spettacolare di processi collegati al furto di informazioni a fini di spionaggio si è avuta nella Germania Federale, uno dei paesi più presi di mira nell'ambito di questa « guerra », agli inizi degli anni '70. In particolare alla fine del 1976 un procedimento penale venne aperto nei confronti di un gruppo di 12 persone che avevano fornito copie di istruzioni di funzionamento di sistemi informatici e di programmi di elaboratore nonché di bande e di dischi ad una organizzazione di servizi segreti dell'Est operante sotto apposita copertura. Gli episodi scoperti sono molto numerosi ed è impossibile citarli tutti giacché, oltretutto, si sono svolti in vari altri Paesi, oltre che in USA e nella Repubblica Federale di Germania, e cioè in Francia, in Canada, in Lussemburgo, nel Regno Unito, ecc. In questi paesi le autorità doganali e giudiziarie hanno intrapreso apposite azioni coinvolgendo anche imprese, a volte di grande notorietà, come ad es. la giapponese Toshiba. Vale forse la pena però di citare quello che gli esperti giudi-

to il sabotaggio di elaboratori di Paesi esteri mediante l'introduzione di « virus » (v. *Expertises*, n. 115 del marzo 1989). D'altro canto, di recente, esperti sovietici hanno dichiarato che studenti stranieri avrebbero introdotto nell'agosto del 1988 dei virus nell'elaboratore dell'Istituto Accademico dei Sistemi di Programma: altri virus sarebbero stati scoperti in altri cinque enti governativi (vedi *Corporate Security Digest* del 26 dicembre 1988).

cano il più clamoroso episodio di spionaggio tecnologico del secondo dopoguerra.

All'inizio del 1984 vennero scoperte a Stoccolma oltre 7.000 bande magnetiche di *computers* che stavano per essere trasferite nell'Unione Sovietica. Le bande vennero prese in consegna dal FOA (Istituto di Ricerca della Difesa svedese) e decifrate dopo un lungo e delicatissimo lavoro dell'equipe tecnica. Vennero così alla luce notizie importantissime sull'organizzazione spionistica dell'URSS in Occidente e particolarmente nella Germania Federale, nonché su segreti militari scoperti dalle organizzazioni spionistiche sovietiche (ad es. i piani relativi all'aereo Tornado). L'Ambasciatore sovietico ed agente principale del KGB, Sig. Pankine, tentò inutilmente di convincere il Premier Svedese dell'epoca, Olaf Palme, pur considerato filosovietico, a consegnare all'URSS le bande: Olaf Palme invece informò della questione il suo gruppo speciale di consulenti e, successivamente, il governo americano e quello tedesco. Il comportamento di Palme non piacque affatto al KGB: fatto sta che qualche tempo dopo, come è noto, il Premier svedese venne assassinato in circostanze ancora non completamente chiarite... Riprendendo il discorso, va rilevato che i Paesi interessati dal fenomeno dello spionaggio tecnologico hanno reagito sia rivitalizzando o modificando il loro « arsenale » giuridico-amministrativo (norme sulla protezione del segreto industriale, scientifico e commerciale, leggi sul diritto d'autore e sulla concorrenza sleale, estensione delle norme penalistiche dirette alla tutela del patrimonio) sia agendo a livello politico-amministrativo.

Nell'ambito internazionale si è cercato poi di stipulare intese commerciali (ad es. tra gli USA ed alcuni paesi asiatici come Taiwan, Hong Kong, Korea, ecc.) ma soprattutto si è fatto ricorso a normative dirette a permettere il controllo sull'esportazione di determinati prodotti di alta tecnologia anche informatica ed, in particolare, sulla loro destinazione finale. Vari Stati (tra i quali gli S.U., il Canada, la Francia, il Belgio, la Norvegia, l'Olanda ed il Regno Unito) hanno emanato disposizioni normative interne al riguardo. Questa attività normativa almeno per i Paesi dell'Alleanza Atlantica e per altri Paesi, tra cui il Giappone, che hanno da tempo aderito ad un organo informale di coordinamento, il COCOM (Coordinating Committee for Multilateral Exports Controls) appare in sintonia con le decisioni di questo Comitato il quale stabilisce periodicamente le liste dei prodotti di alta tecnologia, tra cui quelli informatici, che possono essere forniti ai Paesi dell'Est ed altri Paesi specificamente indicati (ad es. Cuba).

Più di recente alcuni Paesi, come gli S.U., hanno indirizzato la loro politica nel senso di limitare o vietare l'accesso di soggetti o di paesi stranieri alle banche dati nazionali contenenti informazioni tecniche ed economiche, anche se non « classificate », ma ritenute di importanza rilevante ai fini della sicurezza nazionale.

Le regolamentazioni poste in essere, tuttavia, hanno creato situazioni difficili sia all'interno dei vari Paesi Occidentali sia nell'ambito

dei rapporti tra i Paesi membri del COCOM. In particolare, alcune decisioni da parte degli USA di effettuare controlli extraterritoriali sulle apparecchiature informatiche prodotte in USA ma installate all'estero, e di esercitare una specie di supervisione sulla loro cessione, hanno suscitato delicati problemi anche di diritto internazionale.

Per quanto riguarda ora, in particolare l'Italia, il Governo ha presentato alla Camera in data 9 dicembre 1987 il disegno di legge n. 203, recante il titolo « Nuove norme sul controllo dell'esportazione, importazione e transito di materiale di armamento nonché dell'esportazione e transito di materiali di particolare interesse strategico », uno dei quali articoli prevede l'ottenimento di una apposita autorizzazione ministeriale per l'esportazione ed il transito di materiali di particolare interesse strategico utilizzabili a rilevanti fini militari, tra cui (art. 20, lett. 2) *le apparecchiature elettroniche* da indicarsi in un successivo elenco. L'art. 25 punisce con la reclusione da 6 mesi a 5 anni e con multa proporzionale l'esportazione o il transito verso destinazione diversa da quella indicata nell'autorizzazione e, con la sola multa proporzionale, la violazione di altre prescrizioni stabilite nell'autorizzazione medesima.

Particolari disposizioni del codice penale vigente (art. 256, relativo al procacciamento di notizie concernenti la sicurezza dello Stato; art. 257, riguardante lo spionaggio politico o militare, art. 261 relativo alla rivelazione di segreti di Stato, ecc.) permettono di colpire alcune delle attività illegali relative al trasferimento di tecnologia allorché le circostanze del fatto riguardano rapporti politici internazionali. Nei casi normali, invece, allorché si tratti cioè di rapporti tra privati, possono essere applicati, secondo i casi, l'art. 621 (rivelazione del contenuto di documenti segreti), l'art. 622 (rivelazione di segreto professionale), l'art. 623 (rivelazione di segreti scientifici o industriali).

È opportuno sottolineare, riprendendo il discorso generale, che — come hanno ripetutamente affermato esperti del settore — l'acquisizione illegale di tecnologia ha permesso ai paesi del blocco sovietico di risparmiare anni di ricerche e somme ingentissime. Secondo studi condotti in USA e riferiti in Italia dalla rivista specializzata « Informazioni della Difesa » (n. 6/7-1985, p. 31), il risparmio è quantificabile, approssimativamente, in vari miliardi di dollari. Riferisce tra l'altro il detto periodico, che ... « rapporti classificati su sistemi d'arma USA in fase di sviluppo sono stati acquisiti dall'URSS. Essi contenevano informazioni sul radar "vedi in basso/spara in basso" dell'F15, sul radar del bombardiere B1, sul missile aria-aria Phoenix, sul missile SA Patriot, sul missile migliorato Hawk e su un sistema di difesa aerea Nato ».

Secondo gli esperti del Dipartimento della Difesa USA, inoltre, il microprocessore sovietico KR580IK80A è, in realtà, una versione modificata del microprocessore statunitense Inter Corp's 8080A8 mentre l'architettura degli elaboratori IBM 360 e 700 è

stata posta a base della serie degli elaboratori sovietici denominata Ryad.

Paradossalmente, i paesi del blocco sovietico, acquisendo illegalmente tecnologia occidentale, hanno finito per dipendere da questa stessa tecnologia ed in particolare, da quella statunitense: tale situazione da adito a riflessioni che qui per brevità si omettono, ma sulle quali si richiama l'attenzione degli esperti economici e politici dei paesi occidentali.

6. Le risultanze dei *computers* e la prova del reato.

Come ho già detto in altra sede (vedi la mia relazione dal titolo « *Tecnologia informatica e criminalità. Aspetti nazionali ed internazionali* », più innanzi citata) la criminalità, specialmente quella organizzata, sta informatizzandosi sia allo scopo di gestire meglio i propri affari (traffici di droghe, gioco d'azzardo e scommesse illegali, prestiti usurari, sfruttamento della prostituzione, ecc.) sia allo scopo di eludere le indagini della polizia. La scoperta dei relativi schedari informatici ha consentito tuttavia agli inquirenti di ricostruire l'attività criminosa svolta da alcune organizzazioni. Ma non solo la criminalità tradizionale si serve dei *computers*: anche molte attività illegali condotte dagli *white-collars* sono ormai gestite dagli elaboratori. Molto spesso le società si servono del *computer* per gestire la doppia contabilità e soprattutto quella « in nero ». Va detto ora che proprio le risultanze di un *computer* hanno consentito alla Commissione Tower, cioè alla commissione d'inchiesta nominata da Reagan alla fine di novembre del 1986 per studiare le procedure del National Council Security nello scandalo dell'Irangate, di pervenire ad importanti risultati. A monte vi era la « fissazione » di segretezza del Colonnello North il quale, non fidandosi dei telefoni e dei messaggi scritti, aveva fatto installare negli uffici del NSC dei *computers* a circuito chiuso protetti da interferenze esterne e che erano diventati in pratica il sistema esclusivo di comunicazione tra i vari settori, un vero e proprio sistema di posta elettronica (vedi in proposito Newsweek del febbraio 1987 ed il libro di Josca e Platero, *Il Rapporto Tower*, Milano, 1987). I messaggi scambiati tra North e Poindexter furono in seguito cancellati ma rimasero memorizzati nel *central master file* del sistema, senza che di ciò fossero a conoscenza i protagonisti dell'Irangate. La Commissione Tower riuscì a sapere della questione ed entrò quindi in possesso di preziose notizie riguardanti il ruolo dei vari soggetti: come ammettono gli esperti, fu proprio la scoperta dei messaggi e dei documenti memorizzati nel cervello elettronico del NSC a dare una svolta drammatica ai lavori della Commissione. Per la prima volta, come affermano Iosca e Platero, le informazioni contenute in quella « miniera d'oro », consentivano di ricostruire la storia della Iran Connection e di definire, al-

meno in parte, il ruolo e la responsabilità dei protagonisti dello scandalo.

Anche in Italia peraltro le risultanze dei *computers* sono serviti in alcuni casi a mettere nei guai uomini politici ed industriali accusati di gravi reati. È noto l'affare che ha condotto di recente dinanzi la Commissione Inquirente ben 3 ex ministri ed i loro segretari, fondato sui dati contenuti sull'archivio computerizzato di un noto costruttore-faccendiere del Nord nel quale venivano memorizzate le « tangenti » pagate. La stampa italiana inoltre ha dato di recente notizie di una manomissione, sembra involontaria, dei dati contenuti in un *computer* del Ministero dell'Industria e relativi all'elenco di aziende che avevano ottenuto particolari sovvenzioni per la innovazione tecnologica o che aspiravano ad ottenerle, manomissione che avrebbe ostacolato una delicata indagine giudiziaria riguardante la corresponsione di tangenti ad alti funzionari di quel Ministero, mentre i dati contenuti in altro *computer* appartenente ad una ditta coinvolta nelle indagini sarebbero stati manomessi o sottratti da ignoti (i sigilli apposti ai *computers* dagli inquirenti sarebbero stati tolti).

7. Rilievi conclusivi.

L'adozione di specifiche norme, atte a reprimere almeno le forme più gravi di criminalità informatica, è ostacolata a volte nel settore giuridico da coloro che io chiamo gli « ottimisti tecnologici » cioè gli utopisti dotati di incontrollabile fede e « rocciosamente » convinti che il progresso tecnologico è buono *in sé, cioè per definizione*, ed è quindi sempre di segno positivo, in tutti i suoi aspetti ed in tutte le sue implicazioni. Vi è chi si concentra letteralmente su qualcuno degli strumenti tecnologici, come il *computer*, e lo « antropomorfizza », per così dire, finendo per l'attribuirgli — in preda ad un interessante « raptus » di adorazione tecnologica — qualità e proprietà « quasi-umane ».

Si crea in tal modo tra l'essere umano ed il computer un... « legame di sangue » che spinge il primo ad assumere nei confronti del mondo esterno un tipico « ruolo paterno » nei confronti del secondo, ad es. considerando qualsiasi rivelazione di illeciti nei quali il *computer* è in qualche modo coinvolto come un subdolo tentativo di « criminalizzazione » dello stesso.

In realtà si tratta di una vera e propria « reazione viscerale » a quella che viene implicitamente considerata come... una vile aggressione al « pupo ». Un esempio interessante di siffatto comportamento sembra emergere dalla lettura di una recentissima opera di un illu-

stre giurista, schierato ad oltranza tra gli ottimisti tecnologici[10] il quale, tra l'altro, sostiene, in solitario contrasto con una evoluzione ormai irreversibile a livello internazionale e nazionale[11], che non occorrano nuove leggi per combattere il funzionamento della criminalità informatica la cui esistenza, peraltro, è ammessa... sia pure a denti stretti.

Questa presa di posizione appare probabilmente spiegabile se si considera l'atteggiamento formalistico dei giuristi « rétro », profondamente convinti del dogma della completezza assoluta dell'ordinamento giuridico e della possibilità quindi di far ricorso, in ultima analisi, a mitici « principi generali del diritto » per regolare qualsiasi fenomeno che si verifichi nel mondo giuridico. Tuttavia, come già Qualcuno in altra epoca ha affermato... « non si può versare il vino nuovo in vecchi otri ».

Ciò premesso, va rilevato che, in generale, mancano dati statistici completamente affidabili e continuamente aggiornati in ordine all'entità del fenomeno della criminalità informatica ed, in particolare, alla modalità dei fatti, ai danni effettivi arrecati alle vittime, agli esiti dei non molti procedimenti giudiziari iniziati per delitti informatici. La mancanza o la scarsità di questi dati, spesso dovuta alla ben nota riluttanza delle vittime a denunziare i crimini subiti ed a sistemare la questione, per così dire « in casa », impediscono di approntare seri mezzi di prevenzione e favoriscono, in ultima analisi, l'operato dei criminali i quali agiscono spesso con tranquilla impudenza. Il danno non è soltanto « privato », specie allorché le vittime sono rappresentate da società commerciali, da istituzioni finanziarie o, peggio, da enti pubblici: in molti casi, direttamente o indirettamente, la perdita è addossata alla collettività.

Un osservatorio permanente sul fenomeno istituito a livello centrale, ad es. presso il Ministero della Giustizia, consentirebbe di attuare una sistematica raccolta di dati e di tenere desta l'attenzione dei responsabili dei sistemi di sicurezza e dello stesso « top management » nel settore pubblico e privato sui mezzi posti in essere dai nuovi cri-

[10] Vedi di R. Borruso, il volume *Computer e diritto*, II, Milano, 1988, in particolare, p. 345 ss., nota 29. Se il nostro Autore fosse vissuto all'epoca di Aristofane, probabilmente sarebbe stato da questi collocato nella famosa cesta sospesa che compare nella nota commedia dal titolo « Le nuvole... ».

[11] Recentissimamente, il Ministro della Giustizia ha istituito una commissione ristretta di esperti con l'incarico di preparare uno schema di disegno di legge allo scopo di integrare le norme del codice penale in tema di illeciti informatici.

minali per perpetrare i fatti a loro addebitati e, di conseguenza, sui sistemi atti a prevenire o a scoprire in tempo utile i crimini informatici.

La possibilità di stimare in modo affidabile l'entità del fenomeno solleciterebbe molto probabilmente l'attenzione anche dei legislatori e consentirebbe di colmare le lacune più volte lamentate nei sistemi giuridici di fronte ad alcuni particolari tipi di crimini informatici: fornirebbe inoltre alle società di assicurazione elementi utili per predisporre polizze adeguate al particolare rischio. L'attività del proposto osservatorio gioverebbe anche ai fini della specializzazione degli inquirenti, attualmente praticamente inesistente nella maggior parte dei paesi europei. Non basta infatti aver leggi, anche se perfette, se coloro che devono applicarle non sono adeguatamente e tecnicamente preparati ed in grado di comprendere appieno il fenomeno che sono chiamati a combattere. Ci auguriamo che i *decision makers* si rendano presto conto della urgenza di provvedere, secondo una strategia a largo raggio, che contempli iniziative legislative e regolamentari e seri programmi di formazione del personale delle forze di polizia e della magistratura.