GLI ILLECITI INFORMATICI

A proposito di criminalità da «computer»

ENRICO BARAGLI S.I.

«*Telefoni guasti? È uno squalo!*» / «*Un boccone prelibato per i pesci i nuovi cavi sottomarini!*»: questi l'occhiello e il titolo sotto i quali *La Stampa*, il 12 giugno scorso, riportava dal *New York Times* la notizia che gli squali — che sempre avevano sdegnato i cavi sottomarini a fili di rame —, da due anni si andavano mostrando, invece, voraci nei confronti dei nuovi cavi sottomarini a fibre ottiche, tranciandoli con morsi da 250 mila dollari (320 milioni di lire) l'uno. Ragion per cui gli ingegneri dell'*American Telephone and Telegraph* si vedevano costretti a far scendere detti cavi, debitamente corazzati in acciaio, fino a 2.500 metri dove era possibile, e a seppellirli nel fondo marino se vicini a riva.

Ma a palesare, nella fascinosa odierna globale struttura elettronico-informatica, un colosso dai piedi di argilla, non occorreva proprio questa grossolana iniziativa ittica. Da anni, infatti, se n'era incaricata la — spesso criminosa — astuzia degli umani, non tanto manomettendone le connessioni esterne, quanto i suoi cervelli e anime, vale a dire gli stessi elaboratori e banche di dati; dai più potenti (*mainframes*) agli ormai familiari (*home*) e individuali (*personal*) *computer* ipocentri e terminali dell'odierna «civiltà cablata».

Anche in Italia, giornali e rotocalchi, tra l'allarmato e il divertito, ne hanno trattato a iosa [1]. E non meno copiosamente ne è andata trattando l'editoria specialistica, così informatica come criminologico-giuridica. Ne è una prova il volume di M. M. Correra e P.-P. Martucci *I reati commessi con l'uso del computer* [2], che, infatti, in 24 pagine di bibliografia può elencare ben 557 titoli in argomento. Ce n'è, dunque, più che a suffi-

---

[1] Eccone, ad esempio, alcuni titoli a effetto di quest'anno: A. Masia, *Pirata elettronico mischia le bobine: nel caos l'archivio della RAI* (*Corriere della Sera*, 4 apr.), M. Bindi, *Predatori in guanti elettronici* (*La Nazione*, 11 apr.), R. Di Giovacchino, *C'è la rapina in programma* (*Messaggero*, 17 apr.), G. Masini, *Cavalli di Troia anticomputer* (*La Stampa*, 12 mag.).

[2] M. M. Correra - P.-P. Martucci, *I reati commessi con l'uso del computer. Banche dei dati e tutela della persona*, CEDAM, Padova 1986, 266, L. 25.000. Nel testo i rimandi in tondo si riferiscono a questo volume, mentre quelli *in corsivo* si riferiscono all'articolo di P. Di Palma, *Computer crimes*, in *Mass Media* (1987) n. 2, 21-39.

cienza per apprendere che cosa siano gli illeciti informatici, quali e quanti se ne compiano, quali ne siano gli operatori, e quali i — vigenti o auspicabili — deterrenti tecnologici e giuridici.

«Computer crime»?

A una definizione univoca ancora non si è pervenuti. «La stessa OCSE (Organizzazione per la Cooperazione e lo Sviluppo Economico), che se n'è interessata, ci ha rinunciato» (p. *25*). Vero è che la pubblicistica corrente, alla buona, li ha bollati «delitti informatici» (*computer crime*); ma impropriamente, dato che molti di essi non verificano ancora «violazioni dolose o colpose di leggi per cui sia prevista una pena». Solo, dunque, per comodità di discorso passano per *computer crime* «tutti e soli quegli illeciti in cui l'elaboratore elettronico (*hardware* o *software*), o qualcosa ad esso connesso, sia propriamente strumento od oggetto» (ivi).

Primo e più vistoso tra tali illeciti — perché potenzialmente più catastrofico — viene segnalato quello della distruzione o danneggiamento materiale degli stessi elaboratori, specie se *mainframe*. Infatti, in una società che nell'elettronica computerizzata va innervando tutte le sue strutture e mansioni — di produzione e finanziarie, anagrafiche e burocratiche, di trasporti, difesa, polizia, sanità... —, esso può provocare la paralisi (*black out*) di attività e prestazioni sociali più o meno durevoli e vitali, non solo a livello locale e nazionale, ma anche continentali e mondiali. Pure ipotesi? Non proprio.

«Nell'ultimo decennio i crimini di questo genere sono stati numerosi, e talora molto gravi, in diversi Stati occidentali. Negli Stati Uniti, tra la fine degli anni '60 e la metà del decennio successivo, in segno di protesta contro il coinvolgimento del conflitto vietnamita, vi furono diversi e clamorosi attacchi a centri elettronici di elaborazione adibiti a scopi militari. In Gran Bretagna i *computer* della Polizia sono stati ripetutamente presi di mira dai terroristi nordirlandesi dell'IRA. Tuttavia, l'episodio sinora forse più spettacolare è accaduto in Giappone il 29 novembre 1985. Centinaia di estremisti, agendo contemporaneamente a Tokyo e a Osaka, danneggiarono i *computer* e le centraline elettroniche di 7 diverse stazioni ferroviarie, determinando la paralisi dei trasporti della Capitale e bloccando gli spostamenti di 12 milioni di persone. Tra quelli avvenuti in Italia ricordiamo, per l'estrema serietà dei danni, e soprattutto delle conseguenze, l'assalto compiuto a Roma contro i *computer* del Centro Elaborazione Dati della Motorizzazione Civile dalle Brigare Rosse nel dicembre 1981» (p. 26)[3].

---

[3] «Quasi tutti i Paesi industrializzati che conoscono il cancro del terrorismo hanno subito attentati contro i CED (Centri Elaborazione Dati). In Italia, fra il 1975 e il '79 ce ne sono stati una trentina [...]. Per restare all'esperienza italiana, più di una "risoluzione strategica" delle BR si è occupata dei sistemi informatici incitando al sabotaggio dei CED e all'aggressione dei dirigenti di essi. Un manuale delle BR rinvenuto a Roma nell'81 descriveva addirittura sistemi e metodi per sabotare centri elettronici, con un'attenzione particolare a quelli della polizia e dei carabinieri» (p. 24).

Meno vistosi, ma certamente più numerosi e, nell'insieme, poco meno dannosi, gli illeciti perpetrabili sulle operazioni logiche «immateriali» (*software*) delle stesse apparecchiature informatiche (*hardware*). Tali, ad esempio, l'uso, non autorizzato, a proprio utile, delle stesse, mediante chiavi di accesso (*password*) originali, oppure criminosamente contraffatte; la manipolazione dei dati memorizzati, cancellandoli, oppure introducendone di falsi; la duplicazione illegale di programmi con violazione dei rispettivi diritti di autore.

«Utilizzando un *software* di comunicazione e un proprio *minicomputer* collegato all'ordinaria linea telefonica tramite un *Modem* (*Mod*ulatore-*dem*odulatore) è possibile inserirsi nelle reti di comunicazione attraverso cui "colloquiano" i *computer* [...]. Se, invece, il sistema è chiuso, non ha cioè collegamenti col mondo esterno, gli *hackers* (=spaccatori, scrocchiatori, vandali...) potranno accedere innestandosi su una linea collegata a un terminale, o captando le irradiazioni di una trasmissione-dati non schermata [...]. Attraverso combinatori automatici, o con scambi tra di loro, o con particolari abilità personali, gli *hackers* si procurano poi le *password* e i numeri d'identificazione dell'utente. Più spesso, poi, di quanto non si possa pensare, per procurarsi i codici di accesso sfruttano anche la negligenza e la superficialità degli utenti autorizzati» (p. 28).

L'impresa tragico-burlesca con cui due ragazzotti americani, «digitando» il proprio *minicomputer*, riuscivano a far scattare l'allarme nei supercalcolatori del Pentagono su di un imminente conflitto tra URSS e USA — nel 1983 portata anche sui nostri schermi dal film di John Badham *Wargames* (*Giuochi di guerra*) —, non era tutta frutto di fantasia. Altri «colpi», non meno clamorosi, l'avevano preceduta e poi l'hanno seguita, in USA, altrove e anche in Italia.

«Per citare solo alcuni dei tanti casi diventati ormai famosi, ricordiamo quello della "Banda del 414" (prefisso telefonico del Milwaukee): ragazzi fra i 13 e i 17 anni, che nel 1983 riuscirono a penetrare nella banca dati dei laboratori atomici di Los Alamos; quella della banda di ragazzi di San Diego, che riuscirono a modificare alcune parole d'ordine di accesso ai conti della *Chase Manhattan Bank* del Massachusetts impedendo l'accesso ai conti a impiegati e clienti; e quella dei 7 liceali di New York, arrestati nel luglio '85 per avere, tramite i loro *minicomputer*, fatto contrabbando di carte di credito rubate, telefonando gratuitamente in teleselezione intercontinentale, e intercettando numeri telefonici riservati al Pentagono. Conoscevano anche i codici per modificare la posizione in orbita di alcuni satelliti» (p. 26).

«In Italia, il caso più rilevante riguarda la truffa compiuta ai danni dell'INPS nel dicembre 1982, da un operatore economico con la complicità di un impiegato dell'Ente. I due trattennero i contributi pagati da oltre 200 aziende per decine di miliardi di lire, facendoli apparire come versati nel calcolatore dell'INPS» (p. 40).

Non basta. Da qualche anno, anche in Italia, stanno dilagando i furti da «Bancomat», vale a dire le truffe in quel sistema di prelevamento elet-

tronico di valuta che permette ai correntisti di diversi istituti bancari consorziati tra di loro, di prelevare, nei giorni e nelle ore di chiusura degli sportelli, un certo quantitativo di biglietti di banca, mediante una tessera magnetica, digitando un codice segreto noto a ogni singolo correntista. Infatti, molti sono gli illeciti per scoprire detto segreto. Basta, per esempio, sottrarre per pochi minuti al correntista la sua carta e duplicarla con una magnetizzatrice. Né si esclude che, nella pubblica strada, una macchina da presa con tanto di *zoom* filmi i movimenti delle dita di un ignaro cliente sulla tastiera della cassa magnetica (*cash dispenser*)... «Di qui l'obiettiva incertezza psicologica che detti prelievi abusivi vanno generando anche in Italia — dove più di 3 milioni sono gli utenti, serviti da 2 mila sportelli, di 400 banche diverse —; quando si pensi che negli Stati Uniti, già nel 1973, le perdite totali nel settore venivano stimate intorno ai 2.800.000 dollari, e che nel 1982 tali perdite superavano i 45 milioni e mezzo di dollari» (p. 40).

Dalle difese fisiche a quelle giuridiche

Già contro i possibili danni, accidentali o dolosi, imputabili a cause *fisiche* — rischi d'incendi, di allagamenti, di radiazioni e di campi magnetici —, che palesano nell'elettronica informatica un gigante dai piedi di argilla, le misure protettive, anch'esse di tipo fisico, si presentano complesse e costose. Ma molto più complesse e più costose sono quelle *logiche*, a difesa degli accessi logici delle reti e dell'autenticità dei messaggi che passano per le stesse, per impedire cioè la cancellazione o la manipolazione dei messaggi legittimi, e che possano essere duplicati o visualizzati quelli riservati. L'esperienza prova che, in proposito, «la sicurezza assoluta non esiste, e che, comunque, il raggiungerla comporterebbe costi proibitivi» (p. *31*), dato anche il numero e le caratteristiche dei cosiddetti *hacker*, più o meno «delinquenti», che la insidiano.

«Le indagini sinora condotte indicano concordemente che si tratta, nella maggior parte dei casi, di soggetti giovani, dall'età media compresa fra i 24 e i 33 anni, ben preparati nell'informatica, di indole audace e impaziente [...]. Il loro atteggiamento psicologico è decisamente peculiare. In genere essi non ritengono di compiere delle azioni disoneste e contrarie alla legge, ma si considerano piuttosto impegnati a risolvere, provando la propria abilità e intelligenza, dei problemi di ordine logico-scientifico, in modo non dissimile da quanto avviene per i giocatori di scacchi. Questi soggetti operano una netta distinzione fra il danno arrecato alle persone, giudicato immorale e inaccettabile, e il danno causato a un'azienda, che, in determinate condizioni, non ritengono riprovevole [...]. Se, però, in genere i *computer criminals* sono dei dilettanti, senza precedenti penali, esistono sintomi che lasciano intuire il modificarsi di questa realtà. Infatti l'"alfabetismo da *computer*", cioè il numero di persone in grado di padroneggiare questi strumenti, è in continuo aumento. E la stessa criminalità organizzata si va orientando verso reati la cui complessità di preparazione e di attua-

zione è tale da richiedere, o addirittura rendere necessario, l'uso del *computer* per gli stessi motivi per cui esso viene adoperato nelle aziende. Anche secondo gli esperti dell'FBI, che stimano in circa 30 mila i criminali informatici presenti negli Stati Uniti, la delinquenza organizzata sta penetrando in questo settore. Esisterebbero già dei gruppi clandestini, operanti in diverse località americane, con nomi in codice [...], che si aiuterebbero a vicenda nella perpetrazione dei *computer crimes*» (pp. 41-46).

Di qui l'urgenza di difese anche *giuridiche* e, in queste, anche di sanzioni penali, che rafforzino le altre misure di sicurezza. In argomento — a integrare altri contributi già presentati nella nostra rivista[4] — merita di essere segnalato quello più recente, che siamo andati postillando, del docente di criminologia presso la Facoltà di giurisprudenza dell'Università di Trieste, M. M. Correro (collaboratore P.-P. Martucci), inteso «a fornire al lettore, anche se profano, un compendio il più possibile completo rispetto alla vastità dell'argomento» (p. XIV).

Nel testo, il primo capitolo, introduttivo e descrittivo, tratta della diffusione e dell'influsso del *computer* nella società odierna, fornendo anche le informazioni tecniche necessarie per comprendere tutte le tematiche criminologiche, giuridiche e vittimologiche trattate in seguito. Il secondo svolge un'analisi sistematica dei *computer crime*, trattando della loro definizione e classificazione, tecniche e rilevanze, autori e possibili sistemi di difesa. Il terzo «*Computer* e controllo sociale» è dedicato alla tutela della *privacy*, alla legislazione penale italiana, alla disciplina legislativa nel diritto comparato e alla tutela giuridica del *software*. Il quarto e ultimo esamina gli aspetti vittimologici in relazione all'impiego degli elaboratori nel settore della difesa sociale. Seguono, nella seconda e più ampia parte del volume, in altrettante appendici, 13 fra testi originali e completi, di direttive, convenzioni, disegni di legge, estere e italiane, in argomento, e la bibliografia-fiume, già menzionata.

Nelle considerazioni conclusive i due Autori rilevano come, «nella carenza di appropriate norme giuridico-penali, gli autori dei *computer crime*, pur potendo contare su profitti rapidi e ingentissimi, quasi senza confronti rispetto alle fattispecie criminose tradizionali, affrontano rischi estremamente ridotti, sia in termini di eventuale scoperta, sia di entità della pena inflitta» (p. 108). Come non augurarsi che questo loro contributo specialistico valga a ridurre tanto danno contro il bene comune, e a incrementare, invece, tanti frutti, economici e culturali, connessi con un ordinato progresso tecnologico?

---

[4] Cfr E. BARAGLI, *A tutela della «privacy»*, in *Civ. Catt.* 1986 I 246.