

# Il computer "a rischio"

di Angela Carusone

ROMA. Viviamo nell'era dell'informatica, i video-terminali sono ormai di casa ovunque, telematica e microelettronica aprono al mondo nuovi confini. E così come la società si adegua a questa "computer dipendenza", creando nuove professioni e procedendo alla riconversione dei settori industriali e dei servizi, di pari passo si fa avanti un nuovo tipo di criminalità, perpetrata attraverso la manomissione dei sistemi informativi e computerizzati.

In Italia sono ormai divenute famose alcune frodi avvenute utilizzando le carte di credito e alterando i sistemi automatici di cassa continua delle banche. Ma se ne sono verificate sicuramente molte di più; le banche, infatti, per una comprensibile "tutela" della propria immagine, non sempre hanno divulgato i danni provocati da ignoti attaccando i sistemi di elaborazione dati.

Negli Stati Uniti, invece, si è andati anche oltre. Qui, dove è obbligatorio denunciare alle autorità federali i reati commessi manipolando i computer (i cosiddetti "computer crimes") si è venuti a conoscenza di un episodio a dir poco sconcertante: alcuni anni fa un sabotatore — si presume la con-

correnza — modificò i dati di tolleranza relativi alla pompa dei freni di una serie di autoveicoli ed i relativi controlli programmati dalla casa automobilistica produttrice. Solo dopo una lunga catena di incidenti, si riuscì a scoprirne le cause e, conseguentemente, il sabotaggio. La fabbrica fu costretta a ritirare dal mercato tutti gli autoveicoli prodotti e a risarcire le vittime. I danni — solo quelli economici, perchè e chiaramente impossibile valutare le perdite umane o le invalidità — superarono i cinque milioni di dollari.

Ora, lasciando da parte il caso limite della casa automobilistica statunitense, si può notare che i "rischi da robot" sono notevoli. Laddove infatti è avvenuto un sabotaggio poteva verificarsi un guasto. E se il sistema di controllo — computerizzato anch'esso — per una serie di motivi non riusciva ad individuarlo, i risultati non sarebbero stati di molto diversi.

Di questi aspetti, incidenti e crimini realizzati con i computers, e della possibilità da parte delle industrie di assicurarsi contro i rischi che ne possono derivare, si è parlato ieri mattina a Roma, presso il centro di documentazione economica

per i giornalisti. Massimo Penco, amministratore delegato della Ross Collins Italia (una società di brokeraggio assicurativo), ha sottolineato come siano vari e molteplici gli incidenti causati da computers e i modi per frodare attraverso la loro manipolazione. Così come diverse e gravi possono essere le conseguenze per i produttori e per i consumatori.

Per la tutela di questi ultimi il dott. Spigarelli, del ministero dell'Industria, ha ricordato che la Comunità Europea ha emanato il 25 luglio 1985 delle disposizioni sulla responsabilità civile oggettiva riguardo a prodotti difettosi messi in vendita, disposizioni che devono ancora essere recepite e puntualizzate dagli Stati membri. Kit Jones, giovane esperto dei Lloyds di Londra, ha rilevato invece come i "computer crimes" siano invisibili e intangibili oltre che in continuo aumento.

Per questo le società assicuratrici stanno studiando sempre più nuove formule assicurative per coprire i rischi non solo delle banche ma anche degli istituti non finanziari. Un esempio è fornito dalla polizza offerta dalla Ross Collins al settore alimentare, che mette al sicuro da problemi come il ritiro del prodotto.