RAITRE

Riportiamo qui di seguito il testo integrale della nota di Fabio Scaramucci trasmessa dal TG3 del 2 maggio 1985 alle ore 13,45.

Quali strategie di difesa fisica, elettronica ed assicurativa può attuare un'istituzione finanziaria per raggiungere un grado di protezione sufficiente contro la nuova criminalità tecnologica?
È un tema di scottante attualità, di cui si è parlato ieri a Roma nel corso di un convegno che ha visto la partecipazione dei maggiori esperti del settore, italiani e stranieri.

Gli esperti lo definiscono «computer crime», cioè crimine per mezzo di un elaboratore, e con esso ci si suole riferire ad un complesso di attività o azioni illegali che vanno dall'illecito trasferimento di fondi, all'utilizzo in proprio di banche dati, o al trattamento delle informazioni. E il tutto, naturalmente, allo scopo di sottrarre denaro, anche in grande quantità, agli istituti finanziari.
Si tratta di un nuovo aspetto della criminalità, che nasce dalla massiccia diffusione della tecnologia in tutti i settori della vita odierna, e specialmente in quelli del credito e della finanza. Così oggi, accanto ai delinquenti tradizionali che continuano a portare a termine furti e rapine con i consueti mezzi, cominciano ad affacciarsi anche nel nostro Paese i nuovi criminali «tecnologici» che, al posto della lancia termica o di attrezzature simili, ricorrono invece al computer per effettuare le rapine. Ed ecco allora che il computer, da prezioso e spesso insostituibile collaboratore, può diventare un vero e proprio «nemico pubblico» se viene impiegato da persone disoneste. Milioni di dollari, infatti, vengono frodati ogni anno con il suo aiuto.
I più esperti in questo nuovo genere di delinquenza, al momento, risultano essere gli americani (ed è intuibile facilmente il motivo di tale primato, considerando il livello di diffusione di questo tipo di tecnologie negli Usa). Al secondo posto, in questa poco edificante graduatoria, vengono invece gli inglesi. Secondo una statistica dell'Fbi statunitense, i crimini effettuati per mezzo di computer negli Stati Uniti, nel periodo 1978-1983, sono aumentati vertiginosamente, specie quelli dovuti alla trasmissione dati (cresciuti del 43 per cento). Ma soprattutto è risultato che ben l'85 per cento dei casi noti di frode sono state perpetrati da professionisti dell'informatica.
Oggi, del resto, il numero di persone con conoscenze informatiche è aumentato considerevolmente: esiste perciò un largo numero di esperti in questo settore, in possesso delle nozioni sufficienti per portare a termine un atto criminoso. Inoltre, l'uso del computer è divenuto, negli anni, sempre più semplice, mentre i sistemi di controllo realizzati per impedire le possibili frodi non hanno mantenuto lo stesso livello di evoluzione ed aggiornamento.
Il rischio di essere scoperti, insomma, per i delinquenti che impiegano il computer, è decisamente basso, anche per la mancanza di documenti reali che provino il crimine, trattandosi, per la maggior parte dei casi, di transazioni di natura elettronica, che non richiedono l'impiego di carta. Per cui sono gli stessi esperti di sicurezza, sia fisica che elettronica, che, pur avendo da tempo messo a punto sofisticate metodologie di difesa, ammettono che la varietà delle aree di rischio di un sistema di elaborazione è tale che ben difficilmente si potrà coprirle tutte ed in breve tempo. Ecco allora che, per il presente, il completamento della protezione va affidato soltanto ad un'idonea copertura assicurativa, cosa che del resto è costume di molti istituti, specie quelli finanziari.