

# COLLINS NEWS L'Unità

Il rapporto fra computer e criminalità si fa sempre più stretto ed in alcuni casi può diventare un problema di rilevanza sociale

## I «soliti ignoti» degli Anni Ottanta ormai usano l'elettronica per realizzare colpi impossibili

Giorni fa in Francia, al Casinò di Charbonniere, presso Lione, qualcuno ha guadagnato 2 milioni di franchi (circa 400 milioni di lire) ma non con un «en plein», bensì con una sofisticata apparecchiatura elettronica per mezzo della quale venivano comandate a distanza le palline delle «roulettes».

Per mettere a punto questo sistema «tecnologico» di truffa, secondo gli inquirenti, i malviventi devono necessariamente aver fatto ricorso all'aiuto dei 4 o 5 «esperti» internazionali che, in tutto il mondo, risultano essere i soli competenti in questo tipo di «operazioni». La tecnica, infatti, è nota alla polizia francese: i delinquenti penetrano di notte nella sala da gioco, smontano i cilindri delle «roulettes» e vi adattano all'interno un sistema elettronico telecomandato a distanza. La sera successiva, poi, un complice, munito di una microemittente in genere nascosta nella manica del-

la giacca, si apposta presso un tavolo da gioco.

In questo modo, comandando la fuoriuscita di una minuscola puntina d'occluso celata nel cilindro della «roulette» che ferma la pallina sul numero prescelto dai «comparsi» per le loro puntate, in genere molto alte. Al Casinò di Charbonniere la polizia ha scoperto che i cilindri truccati erano tre, e vi è la «convincione che questa «gang» operi anche in altre case da gioco francesi ed europee.

### La truffa del telex

E veniamo all'Italia. Nella sede centrale di un istituto bancario, a Napoli, arriva una telefonata anonima che comunica la presenza di una bomba. La sede viene immediatamente evacuata, ma da una macchina telex abbandonata nella sala estero viene inviato un messaggio di

bonifico per 500 milioni di lire su una banca tedesca. Il denaro, in Germania, viene prelevato il giorno stesso.

Di episodi simili, negli ultimi anni, sembra ne siano avvenuti parecchi, anche se le banche hanno evitato di denunciarli per ragioni di prestigio. Si calcola comunque che le sole banche italiane abbiano subito in questo modo furti per circa 300 miliardi di lire, con una incidenza progressiva, tanto da prevederne un aumento stimato intorno agli 80 miliardi solo per quest'anno. In Francia, invece, si dovrebbero raggiungere, sempre nell'85, i 130 miliardi e negli Stati Uniti addirittura i mille miliardi.

Gli esperti lo definiscono «computer crime», cioè crimine per mezzo di un elaboratore, e con esso ci si vuole 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, spesso in grande quantità, agli istituti finanziari e di credito.

Si tratta di un nuovo aspetto della criminalità, che nasce dalla massiccia diffusione della tecnologia in tutti i settori della vita odierna, e specialmente, appunto, 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 a prendere piede anche nel nostro Paese i nuovi criminali «tecnologici» che, al posto della lancia termica o di attrezzature simili, ricorrono invece al computer per effettuare i loro «colpi». Ed ecco allora che il computer, da prezioso e ormai quasi 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 genere di delinquenza, al momento, risultano essere gli americani, ed è facilmente intuibile 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 stati perpetrati da professionisti dell'informatica.

Oggi, del resto, il numero di persone con conoscenze informatiche è aumentato in modo considerevole: esiste perciò un largo nu-

mero di esperti in questo settore, in possesso delle nozioni sufficienti per portare a termine un atto criminale. 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.

### Pochi i rischi

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 stesso. Inlandandosi, per la maggior parte dei casi, di transazioni che avvengono per via elettronica e che quindi non richiedono l'impiego della carta. Per cui sono gli stessi esperti di sicurezza, sia fisica che elettronica, che, pur aven-

do 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 coprire tutte ed in breve tempo.

Ecco allora che, per il presente, il completamento della protezione va affidato soltanto ad un'adeguata copertura assicurativa, cosa che del resto è costume di molti istituti, specie quelli finanziari. I Lloyd's di Londra, ad esempio, hanno studiato un tipo di polizza che garantisce la copertura assicurativa contro i rischi del «computer crime»: denominata «ccc» (computer crime coverage) ed offerta in Italia dalla Ross Collins, costa 200 milioni all'anno e copre fino a 10 miliardi. Al momento sono già 7 le banche italiane ad averla sottoscritta, ma si prevede una ben più ampia diffusione nei tempi brevi.

Fabio Scaramucci