PAOLO BERNASCONI

LA PREVENZIONE DEL *COMPUTER CRIME* NEL SETTORE BANCARIO (L'ESPERIENZA SVIZZERA)

SOMMARIO 1. Casi tipici di manipolazioni abusive. — 2. Indicazioni statistiche. — 3. Le soluzioni del diritto penale svizzero. — 4. L'integrazione delle misure di sicurezza. — 5. Denuncia penale: i pro e i contro. — 6. La consulenza esterna. — 7. Conclusione. — 8. Allegati: I. Casistica giudiziaria svizzera e straniera. — II. Norme penali vigenti. — III. Norme penali proposte. — IV. Testo del progetto di revisione.— V. Bibliografia. — VI. La banca-dati della criminalità-informatica.

È ormai divenuto un luogo comune rammentare che il punto più sensibile di una banca non è più la sua cassaforte bensì il suo centro elettronico. Con questo si vuole attirare l'attenzione dei responsabili verso i rischi insiti nella diffusione dell'informatica. « Hackito ergo sum » sembra essere divenuta la massima di numerosi capaci ed appassionati operatori informatici, stimolati ad una sfida permanente verso le macchine affidate alla loro maestria. Non rimane che appellarsi ad una maggiore autodisciplina interna ad ogni impresa economica. Ne è presupposto la conoscenza del fenomeno negativo che s'intende prevenire, come pure dei mezzi tecnici disponibili per attuare un sistema di sicurezza.

1. Casi tipici di manipolazione abusive.

Il principio « meglio prevenire che guarire » è divenuto proverbiale. Nella criminalità informatica acquista una portata ancora maggiore che in altri settori poiché la guarigione è resa più difficile che altrove a causa della quasi impossibilità di scoprire per tempo le ragioni della « malattia », ossia gli abusi. L'informatica infatti, offre i suoi formidabili servigi a chiunque la sappia utilizzare. Pertanto, anche l'operatore disonesto può trovarsi un alleato molto prezioso. Ba-

* Relazione aggiornata, presentata al 4° Congresso internazionale « Informatica e Regolamentazioni giuridiche » organizzato dal CED-Corte di Cassazione, Roma 16-21 maggio 1988.

stino alcuni convincenti esempi: il *computer* permette di operare anche a lunga distanza (in particolare grazie al EFTS/*Electronic Funds Transfer Systems*) in modo da poter perfezionare l'operazione abusiva sfruttando il periodo che intercorre fra la sua esecuzione e la sua verifica.

Per questa ragione i giorni preferiti per simili malversazioni rimangono quelli immediatamente precedenti quelli festivi e preferibilmente quelli lavorativi in un paese e festivi nell'altro: per esempio, è conosciuta una truffa effettuata nell'ottobre 1984 mediante un falso ordine di bonifico per 4 milioni di dollari fatto partire dagli USA in direzione della Svizzera. Quando da parte della banca svizzera destinataria venne chiesta la conferma, in Svizzera era un giorno lavorativo mentre a New York si festeggiava il *Columbus Day*, per cui il *computer* confermò la regolarità dell'operazione, ciò che non sarebbe avvenuto se fosse stato presente un funzionario. Una truffa simile venne commessa in occasione del *Thanksgiving Day*. In secondo luogo, il *computer* permette di programmare l'esecuzione di un reato anche a distanza di tempo, magari in un'epoca in cui l'operatore disonesto non è più alle dipendenze dell'azienda scelta come vittima, alla quale sarà quindi ancora più difficile risalire all'autore. Inoltre il *computer* permette l'esecuzione di malversazioni anche di entità così ridotte da non dare nell'occhio, che però fruttano ingenti profitti all'autore poiché il *computer* le può ripetere per un numero praticamente illimitato di volte. Ci riferiamo ai noti casi dell'accredito sul conto dell'autore di frazioni di centesimo corrispondenti agli arrotondamenti effettuati sul calcolo degli interessi dei conti dei clienti di una banca oppure sul calcolo degli stipendi dei dipendenti di una grande ditta. Infine, il *computer* permette anche di cancellare le tracce del reato, in modo che non si possa più risalire all'autore dello stesso né ricostruire il *modus operandi* così in fretta da riuscire a ricuperare la somma sottratta. Anzi, si conosce persino il caso di chi è riuscito a « catturare » il password di un collega, utilizzandolo per una malversazione, in modo da depistare le indagini verso quel collega. Di fronte a tante difficoltà nella scoperta dell'autore di abusi informatici non si può che sottoscrivere questa conclusione ormai acquisita nella revisione bancaria:

« The more general view today is that the internal auditor's interest is in fraud prevention rather than in fraud detection ».

2. Indicazioni statistiche.

La diffusione della criminalità informatica ha preso dimensioni tali da divenire oggetto della cronaca quotidiana[1]. A questo punto non

[1] Brink V., *Modern Internal Auditing*, New York, 1973.

rimane altro che chiedersi se sono attendibili le cifre astronomiche che vengono propinate al pubblico in relazione ai danni materiali cagionati annualmente da questo fenomeno all'economia di un paese. Da un lato siamo inclini alla prudenza, poiché quasi sempre si tratta di valutazioni e non del risultato di constatazioni di fatto. D'altro lato però, le rare inchieste condotte sul campo tendono piuttosto a confermare almeno l'ordine di grandezza delle valutazioni più allarmistiche. Di fronte alle note carenze statistiche in questo settore non ci rimane che proporre un elemento di riflessione relativo alla Svizzera. Dal 1982 il Cantone di Zurigo allestisce statistiche riguardanti il danno complessivo cagionato dai reati economici scoperti nel Cantone dalle sue autorità giudiziarie[2]. La cifra oscilla fra i 200/300 milioni all'anno. Le rilelevazioni condotte in alcuni degli ultimi anni dalla Procura Pubblica riguardo alla giurisdizione del Sottoceneri (Lugano e Chiasso) hanno stabilito un danno annuo oscillante attorno ai cento milioni di franchi[3]. Non è d'altronde azzardato ritenere che livelli simili siano stati ottenuti anche sulle piazze finanziarie di Ginevra e Basilea.

Vi sono poi da aggiungere ancora i casi scoperti sulle altre piazze secondarie, dove pure ogni anno vengono celebrati due o tre processi di grande mole. Pensiamo anzitutto a Losanna, Zugo, Berna, San Gallo, Lucerna e Coira. In questo modo è possibile stimare in circa un miliardo il danno totale cagionato ogni anno in Svizzera dai reati economici che sono stati scoperti e denunciati alle autorità penali.

Non in tutti, ma nella gran parte di questi casi, l'abuso del *computer* ha costituito lo strumento principale oppure secondario per la consumazione del reato o per l'occultamento del provento del reato. Pur esprimendo tutte le debite riserve di fronte ad una rilevazione così sommaria ed empirica, si deve giungere anche per la Svizzera agli ordini di grandezza che vengono espressi anche per quei paesi in cui l'informatica si è diffusa con la medesima portata e per i quali si dispone di statistiche o stime, come gli USA e la Repubblica federale tedesca[4].

[2] KRISTA, *Kriminalstatistik des Kantons Zürich*, Hrsg. Kantonspolizei Zürich, 1982-1986.

ZIMMERLI ERWIN, *Wirtschaftskriminalität - Tat, Täter*, Opfer-Eine empyrische Untersuchung, 1983-1985, Zürich, 1986.

[3] Rendiconto del Procuratore Pubblico Sottocenerino per l'anno 1978 e 1984 (pubblicato nel rendiconto del Consiglio di Stato per l'anno 1978 e 1984).

[4] Alcuni dati statistici contenuti in uno studio dell'American Bar Association sono riprodotti in the OECD Observer, n. 142 September 1986, p. 20.

Per la RFT cfr. P. PORTING-E. POTT, *Computerkriminalität-Ausmass, Bedrohungspotential Abwehrpotential Abwehrmöglichkeiten*, Wiesbaden, 1986.

Per la Svizzera cfr. H. EGLI, *Grundformen der Wirtschaftkriminalität, Fallanalysen aus der Schweiz und der Bundesrepublik Deutschland*, Heidelberg, 1985, p. 145 ss.; G. ANTOGNAZZA, *Computerkriminalität: Stellenwert überschätzt*, Kriminalistik, luglio 1983; A. BRANDT, *Die grössten Computerbetrugsfälle*, in *Schweizer Treuhänder* (2/78).

Ma quel che ci preme maggiormente di fronte ad ogni statistica riguardante la criminalità informatica è far presente in tutta la sua importanza il problema della cosiddetta « dark figure ». In generale in tutti gli studi di criminologia viene formulato il sospetto che la quota dei casi non conosciuti sia molto più elevata in questo settore che negli altri settori della criminalità. Ciò è dovuto alle ragioni seguenti: la difficoltà di scoprire questo tipo di reato, il fatto che gran parte dei casi scoperti rimangono sconosciuti, poiché le vittime, specialmente nel settore terziario, preferiscono regolarli internamente senza rivelarli all'esterno e nemmeno alle autorità penali; in terzo luogo, queste ultime non in tutti i paesi perseguono sistematicamente questi casi, sia per carenze nella propria legislazione penale che per carenze nel proprio apparato d'inchiesta; infine, non tutti i casi denunciati figurano nelle statistiche nazionali, i cui sistemi divergono ancora da un paese all'altro.

Secondo le valutazioni criminologiche più autorevoli[5] la situazione si presenta oggi come segue: un centro elettronico ogni 40 è oggetto di un abuso, solamente l'1% degli abusi vengono scoperti e solamente un autore di abuso informatico su 22.000 viene punito penalmente. Aggiungiamo ancora che l'abuso informatico è quello che, in media, rende di più finanziariamente rispetto agli altri tipi di reato economico, ciò che è dovuto al valore elevato dei dati affidati al *computer*, alla facilità di continuare a delinquere indisturbati anche per un periodo di tempo prolungato, alle possibilità offerte dal *computer* medesimo di accumulare operazioni in misura elevatissima ripetendo migliaia di volte la stessa operazione abusiva. Infine, il *computer* offre persino la possibilità di sottrarre anche di più di quanto sia contenuto nella disponibilità patrimoniale della vittima, grazie al fatto che si possono sempre creare valori fittizi: da una cassetta di sicurezza è possibile sottrarre soltanto ciò che vi è contenuto, mentre manipolando su un terminal anche di una piccola succursale bancaria è possibile ottenere l'esecuzione abusiva di un ordine di pagamento che supera di parecchi multipli quanto esiste nella cassa di questa succursale.

A questo punto abbiamo accumulato sufficienti spiegazioni per giustificare questa affermazione di R. Fane del MIT:

« If I were a professional crook, I would do it with computers these days ».

[5] U. SIEBER, *The International Handbook on Computer Crime*, New York, 1986, p. 29.

3. LE SOLUZIONI DEL DIRITTO PENALE SVIZZERO.

Anzitutto, una premessa di metodo: per tenere conto dell'ambito precisamente delimitato dei problemi in discussione nell'incontro odierno, ossia quello dei servizi bancari, presentiamo una serie di casi svizzeri e stranieri (annesso I) ristretti alle manipolazioni abusive. Pertanto non vengono presentati casi rientranti nelle altre tre categorie tipiche della criminalità informatica economica, ossia: lo spionaggio, la sottrazione di tempo informatico ed il sabotaggio. Parimenti non vengono qui considerati altri aspetti[6], che non possono però essere dimenticati nella valutazione di un sistema di prevenzione, ossia i principi e la legislazione riguardanti da un lato la protezione dei dati come parte integrante della tutela della privacy e, d'altro lato, la protezione della proprietà intellettuale (diritto d'autore, marchi di fabbrica, brevetti, ecc.). Nella discussione odierna viene quindi utilizzata una definizione più restrittiva di *computer* crime rispetto a quella stabilita dall'OCSE nel suo studio del 1983; che è però necessario ricordare: « Any illegal unethical or unauthorized behaviour involving automatic data processing and/or transmission of data »[7]. Fatta questa premessa di metodo occorre rammentare che nel diritto penale svizzero non esistono norme speciali riguardanti esclusivamente la criminalità informatica.

Attualmente si deve ancora fra capo alle norme del Codice penale svizzero e di altre leggi federali, sotto le quali cadono una gran parte delle malversazioni informatiche. Sino ad oggi, i tribunali si sono infatti sforzati di fare rientrare queste nuove forme di criminalità economica sotto le norme vigenti. Le principali forme di reato vengono esposte nello schema dell'annesso II. Allo scopo di colmare le lacune vigenti alcune nuove norme saranno introdotte nel Codice Penale (cfr. l'annesso III). Si tratta in particolare della truffa informatica, della falsificazione di dati registrati su supporti magnetici e simili nonché del furto di tempo informatico. Queste proposte sono contenute nell'avamprogetto di revisione dell'intero capitolo dedicato alla criminalità economica del Codice Penale, che venne presentato nell'agosto 1985 da parte di una commissione federale di esperti. In generale, nel corso della procedura di consultazione presso i Cantoni, i partiti politici e gli altri enti interessati, queste proposte hanno incontrato una eco favorevole, per cui ci si può attendere che faranno oggetto di una proposta di revisione parziale del Codice Penale che dovrebbe essere sottoposta al Parlamento nel corso del 1989.

La revisione dovrebbe ovviare alle lacune seguenti, almeno per quel che concerne la criminalità informatica:

[6] M. LOSANO, *Corso d'informatica giuridica*, Torino, 1984-1986.

[7] OCSE, *Computer-related Criminality: Analysis of Legal Policy in the European Area*, Parigi, 15 novembre 1984 DSTI/ICCP 84.22.

a) da un lato, il reato di truffa presuppone un inganno nei confronti di una persona, mentre, mediante l'abuso informatico, è la macchina ad essere ingannata. Pertanto l'indebito rimane impunito, ma esclusivamente a condizione che il profitto venga conseguito senza che da parte della vittima vi sia stata nessuna partecipazione. Attualmente questo caso è ancora raro: si verifica però quando l'utente disonesto riesce ad ottenere una prestazione in modo esclusivamente automatico, come per esempio ai distributori di benzina attrezzati con il cosiddetto « ec-direct system » oppure ai distributori di denaro contante (bancomat, postomat) come pure alle cabine telefoniche a pagamento mediante carta di credito personale. In questi casi si potrebbe però ipotizzare il reato di furto[8]. Per contro, nei sistemi non ancora completamente automatizzati, nei quali cioè in determinati stadi dell'operazione vi è ancora un intervento umano, permane applicabile l'art. 148 cod. pen. per la truffa.

b) D'altro lato, il reato di falsità in documenti presuppone l'esistenza di uno scritto (in base all'art. 110 cod. pen.) e, di conseguenza, di un supporto sul quale si possa tracciare un segno scritto. Poiché il supporto magnetico non corrisponde a questo requisito obiettivo, la dottrina è sempre stata generalmente dell'avviso che la falsificazione di dati elettronici non potesse cadere sotto l'art. 251 cod. pen. che attualmente punisce la falsificazione di documenti.

Di diverso avviso è stato il Tribunale federale che, in una ormai famosa sentenza[9], ha sconvolto questa posizione, dichiarando punibile per falsità in documenti l'inserimento nel *computer* di dati non corrispondenti alla realtà. Ma una lacuna sembra permanere comunque nella legislazione penale vigente, per quei dati che possono essere letti solamente da una macchina, come il caso delle carte cosiddette « intelligenti » del tipo PIN (Personal Identification Number) o simili. Una nuova norma che colmi questa lacuna è importante in vista della diffusione dei sistemi di vendita con addebito diretto sul conto del cliente del tipo POS risp. EFTPOS (Electronic Funds Transfer at the Point of Sales).

[8] In questo senso N. SCHMID, *Die strafrechtliche Erfassung von Missbräuchen im Bereiche des Bargeldlosen, insbesondere elektronisch abgewickelten Zahlungs-und Kreditverkehrs*, conferenza tenuta al corso d'istruzione della Società Svizzera di diritto penale, Zurigo, 24 ottobre 1986 in *Schweizerische Zeitschrift für Strafrecht*, 104 (1987), 131, 159. Cfr. anche F. WOLFFERS, *Computerkriminalität: Schärfere Strafbestimmungen gegen EDV-Täter*, Output 7, 1986.

[9] Cfr. STF 111 IV 119 (fattispecie descritta al caso n. 1, All. I).

c) Inoltre, una nuova norma (art. 148 del suddetto avamprogetto) dovrebbe colmare la lacuna attualmente esistente[10] riguardo a determinati abusi delle carte di credito[11].

4. L'INTEGRAZIONE DELLE MISURE DI SICUREZZA.

Riguardo alla sicurezza nell'informatica siamo usciti solo da qualche anno dalla preistoria. Non è lontana l'epoca in cui chiunque poteva accedere indisturbato ai locali in cui era installato un centro elettronico di una banca. Oggi tutti sono convinti della necessità di adottare misure di sicurezza. Ma vi è un ulteriore principio fondamentale del quale oggi è necessario convincersi: ogni misura di sicurezza deve essere integrata in un sistema globale di sicurezza[12]. In caso contrario la sua efficacia viene di molto diminuita quando non addirittura annullata. Siamo entrati quindi in un'epoca dominata dal motto « la misura di sicurezza è pericolosa ».

Questo motto a prima vista sembra azzardato. In realtà appare molto più indicato di quanto sembri, non appena precisiamo che stiamo parlando della pericolosità della misura di sicurezza isolata. Infatti, l'adozione di una singola misura di sicurezza ingenera di solito un atteggiamento quasi fideistico di acquisita immunità. L'esperienza insegna invece che una sola misura di sicurezza di per se stessa non è mai sufficiente e che, inoltre, essa deve in ogni caso essere sottoposta sia al controllo della sua osservanza e della sua efficacia sia all'aggiornamento di fronte all'evoluzione delle nuove tecniche inventate dal delinquente informatico.

D'altra parte, però, anche la sicurezza rappresenta un settore che richiede elevata specializzazione. Per la direzione di un'azienda non è sempre agevole verificare se una proposta o la sua realizzazione raggiungono lo scopo desiderato. Pertanto, offriamo un elenco di domande elementari che devono essere poste a colui che propone un nuovo modello di sicurezza, sia esso il venditore di un programma informatico sia esso il responsabile interno della sicurezza nell'azienda. Oltre alle domande sui costi e sui tempi di messa in esercizio eccone alcune supplementari relative alla efficacia:

[10] Il Tribunale federale ha dichiarato non punibile l'abuso di carta di credito da parte di persona insolvibile ed avente il conto scoperto (STF 110 IV 20 ss. 111 IV 135, STF non pubbl. del 27 agosto 1986, STF 112 IV 79).

Parimenti non punibile venne giudicata l'utilizzazione di assegni Eurocheque scoperti a condizione che l'importo incassato non superi i Fr. 300 per ogni assegno (STF non pubbl. 13 novembre 1986). Cfr. anche in *Praxis* 76 (1987) Nr. 12.

[11] Contro la necessità di una nuova norma in tal senso si è pronunciato M. BUSER, *Straftaten im Zusammenhang mit Kreditkarten, Abhandlungen zum Schweizerischen Recht*, Heft 505, Berna, 1986.

[12] H. LUTZ, *Criminalité economique et revision interne*, in *Collection revision bancaire*, Institut d'economie bancaire de l'Ecole des Hautes Etudes de St. Gall. 1980, p. 135.

a) la misura di sicurezza è già stata verificata su un modello concreto simile a quello in cui dovrà essere introdotta?

In altre parole, è meglio evitare che sia la propria azienda a fare da cavia nella sperimentazione di un prototipo. Se la misura è già stata sperimentata, se ne devono esigere i risultati come pure le eventuali misure supplementari che si sono rese necessarie dopo i primi risultati.

b) La misura di sicurezza proposta può essere periodicamente verificata riguardo alla sua efficacia una volta messa in funzione?

c) La misura di sicurezza è accompagnata dai dispositivi di protezione utili per neutralizzare eventuali contromisure dirette? Se la misura di sicurezza è costituita, per esempio, dall'introduzione del password, si dovranno esaminare misure di autoprotezione, come per esempio:

ca) l'elaborazione elettronica del password con modifica automatica periodica;

cb) la possibilità di un doppio password, per i dati e le operazioni particolarmente sensibili, analogamente al sistema della doppia firma per le operazioni documentali;

cc) la possibilità di fornire, anche al titolare di password, dati in codice, decifrabili soltanto mediante l'utilizzazione di sistemi (per esempio DES - Data Encryption Standard) accessibili a gruppi ancora più ristretti di operatori;

cd) la possibilità di una verifica automatica della legittimità dell'operatore che si è inserito nel sistema mediante password (per esempio mediante il CHAPS-Clearing Automated Payment Scheme);

ce) la possibilità di stabilire immediatamente l'identità di chi ha effettuato ogni operazione e a partire da quale terminale.

d) La misura di sicurezza proposta è integrata nel sistema di misure di sicurezza immediatamente circostante (microsistema)? Rimanendo ancora all'esempio dell'introduzione del password, il suo « microsistema » di sicurezza è costituito dall'insieme delle misure riguardanti l'intero centro di elaborazione elettronica dei dati. Per esempio le misure di carattere edilizio per impedire l'accesso ai non autorizzati oppure le misure nella scelta del personale (tenendo presente che ormai, l'estratto del casellario giudiziale serve a poco, perché i delitti informatici o non vengono scoperti o, quando lo sono, soltanto raramente vengono denunciati penalmente, in modo da condurre ad una condanna e, infine, all'iscrizione nel casellario).

e) Il sistema di sicurezza immediatamente circostante alla misura di sicurezza proposta (microsistema) è a sua volta integrato nel sistema globale di sicurezza dell'azienda? (macrosistema).

A questo punto basta rinviare alle regole generali di sicurezza[13], fra le quali menzioniamo:

[13] T. FISCHER, *Computerkriminalitäet, Gefahren und Abwehrmassnahmen*, Berna, 1979, p. 29 ss.; AA.VV., *Revision du traitement electronique des informations dans les*

ea) il principio fondamentale della separazione delle funzioni: ancora troppe volte si constata che è il programmatore ad essere incaricato di elaborare il programma di sicurezza da applicare alla sua attività e, persino, di spuntare e far quadrare le differenze evidenziate proprio dal programma di sicurezza;

eb) l'istruzione del personale, specialmente riguardo all'esistenza di alcuni settori di rischio particolare, come quelli in cui si lavora abitualmente con provvigioni alla clientela, con pagamenti in contanti, con operazioni monetarie internazionali di contrabbando oppure utilizzando persone giuridiche che hanno sede nei cosiddetti paradisi fiscali. Queste società, molto diffuse perché molto adatte per l'evasione fiscale, sono però anche quelle che sempre vengono utilizzate nei più gravi casi di criminalità informatica. Il personale deve quindi essere informato sul fatto che in determinati paesi è possibile costituire una banca o una società commerciale con nome e capitale sociale dichiarato altisonanti anche se in realtà basta limitarsi a pagare una tassa di pochi dollari;

ec) la sorveglianza accresciuta dei settori in espansione esplosiva: la concentrazione di malversazioni proprio nei settori in rapida espansione — perché di solito sono i più produttivi a corto termine — raccomanda particolare prudenza. Basti pensare alle frequenti disavventure nei settori divise, materie prime e metalli preziosi dove anche in Svizzera si verificarono alcune delle più colossali perdite bancarie: 222 milioni cagionati da un cambista trentenne presso la filiale di Lugano della Lloyd's Bank International nel 1974 e 700 milioni cagionati presso la Woshkod Bank di Zurigo nel 1985 dal responsabile trentaseienne del settore divise.

Il sovraccarico di lavoro in questi settori fa saltare tutte le misure di sicurezza. Ad esempio, i superiori tollerano il mancato rispetto delle norme interne scritte. Poiché si accumulano ritardi a livello della registrazione delle operazioni giornaliere l'operatore disonesto ha la possibilità di tenere aperte operazioni rischiose o vietate più a lungo di quanto sia permesso dai regolamenti interni. In tale caso, anche una misura prudente come l'obbligo di una *fiche* — numerata e con timbro orario — per ogni operazione, perde la sua efficacia. La perde anche se — come talvolta ancor'oggi si constata — la registrazione viene affidata al personale dello stesso reparto invece che a quello di un altro, in ossequio al sempre fondamentale principio della separazione delle funzioni.

etablissements de crédit, Collection Revision Bancaire, Institut d'Economie bancaire de l'Ecole des Hautes Etudes de St. Gall, 1980, AA.VV., *Guide de l'audit informatique*, CLET, Paris, 1985. A. Biasiotti, *La sicurezza dei dati e il computer crime*, in *Bancamatica*, agosto 1986, p. 15.

5. Denuncia penale: i pro e i contro.

Nel sistema generale di prevenzione di un'azienda rientra anche l'elaborazione di una strategia riguardo ai rapporti con l'autorità giudiziaria penale. Trattandosi di una casistica molto differenziata, è improduttivo tentare di stabilire una scelta *a priori* fra le due posizioni estreme, ossia quella consistente nel denunciare tutte le irregolarità penalmente reprensibili e quella consistente nel non presentare mai nessuna denuncia. Pur mantenendo la dovuta elasticità di fronte ad ogni singolo caso, dall'esperienza è possibile ricavare alcune considerazioni sicuramente utili.

Si deve anzitutto partire dal presupposto che l'azienda rimasta vittima di un'irregolarità ha il massimo interesse di chiarirne tutti i risvolti aprendo un'indagine. L'indagine è finalizzata a questi obiettivi: in primo luogo coprire il danno materiale subito, sia ricuperando i beni sottratti sia ottenendo un risarcimento corrispondente, in secondo luogo prevenire un danno materiale ulteriore, sia bloccando un reato ancora in corso (cfr. i casi *sub* cifra 9 e 10 nell'annesso I) sia impedendo, mediante il rafforzamento delle barriere esistenti, che lo stesso sistema abusivo possa essere di nuovo utilizzato. Per raggiungere questi obiettivi è necessario che l'indagine riesca a stabilire almeno l'autore del reato ed i suoi complici all'interno e/o all'esterno dell'azienda, il *modus operandi* (con particolare riguardo ai metodi utilizzati per aggirare le eventuali misure di sicurezza esistenti) e le vie utilizzate per far scomparire il bottino.

Questa indagine viene solitamente affidata all'ispettorato interno, eventualmente con la collaborazione dell'ufficio di revisione bancario, e dei fornitori dell'impianto ED e dei relativi sistemi di sicurezza, a seconda della difficoltà dell'inchiesta e dell'entità del danno da coprire. Si tenga conto però che generalmente questa inchiesta può condurre a buoni risultati solamente se viene affidata a specialisti in informatica che siano integrati in un team comprendente persone cognite dei problemi speciali del settore colpito come pure un giurista. Rispetto all'autorità giudiziaria un team del genere può probabilmente vantare una maggiore competenza tecnica, ma è però svantaggiato riguardo ai mezzi disponibili. Infatti, soltanto l'autorità giudiziaria dispone dei mezzi coercitivi che permettono di estendere le indagini anche all'esterno dell'azienda rimasta vittima di un reato informatico. Si tratta di mezzi previsti dalla procedura penale che non possono assolutamente essere esercitati, per loro stessa natura, da parte dei privati: la perquisizione nei luoghi sospetti, come l'abitazione del sospettato, gli uffici di suoi eventuali complici, le cassette di sicurezza presso altre banche intestate a persone fisiche o giuridiche vicine alle persone sospettate, come familiari, fiduciari, amici, consulenti, e simili.

Il sequestro permette di acquisire documentazione probatoria nascosta dall'autore come pure di bloccare il provento del reato, non solo in Svizzera ma anche all'estero. L'autorità penale ha pure la facol-

tà di ottenere informazioni presso altre banche senza che possa essere opposto il segreto bancario. Infine, l'interrogatorio delle persone sospettate come pure di altre persone nella veste di testimone può essere condotto in modo e in tempi che permettono di scoprire la verità, in tutto o in parte. Per esempio, l'autorità penale ha la possibilità di procedere all'audizione di più persone contemporaneamente, in modo da evitare che vengano concertate delle versioni inveritiere. Spesso queste semplici tecniche, come pure il fattore sorpresa, hanno permesso di chiarire casi sui quali avevano invano indagato, senza successo, anche per parecchi mesi, team d'ispettori interni.

Naturalmente, l'importanza e la difficoltà del caso forniranno indicazioni per stabilire fino a che punto e a che momento debbano essere estese le indagini interne e a che momento debbano essere sospese per fare intervenire le autorità penali. A questo riguardo, il criminologo tedesco Sieber suggerisce quanto segue:

« The decision concerning legal actions and the evaluation of the available evidence should only be made in cooperation with a legal adviser who has special knowledge of the issues » (*op. cit.*, p. 137).

Quando la vittima di un reato economico è una banca oppure una società finanziaria oppure uno o più dei loro clienti, la decisione se sporgere denuncia o meno è condizionata dal timore che possa essere rivelata l'identità del cliente coinvolto oppure di clienti coinvolti inconsapevolmente. In generale, l'autorità penale svizzera è sufficientemente sensibilizzata a questa problematica, anche riguardo alla clientela residente all'estero, per cui ha elaborato una serie di meccanismi che, senza intralciare il regolare corso dell'inchiesta né i diritti delle parti, permettono di tutelare in modo soddisfacente quando non assoluto l'identità della clientela. Ecco alcuni esempi concreti: il nome del cliente non viene mai menzionato negli atti (verbali, decreti, atto d'accusa, sentenze, ecc.) una volta che la sua identità è stata accertata dal magistrato competente (Procuratore Pubblico, Giudice Istruttore, Presidente della Corte). Il suo nome viene conservato a parte, in modo che non venga a conoscenza di tutte le parti che hanno diritto di visionare gli atti processuali; in casi estremi, anche nel verbale d'interrogatorio del cliente sarà omesso il suo nome, al posto del quale figurerà il numero o la sigla usata per il suo conto bancario. Il nome, ed eventualmente la fotocopia del suo documento d'identità, viene menzionato in un atto separato da aprirsi soltanto per comprovate necessità istruttorie. Del resto, è noto che anche nel dibattimento pubblico nei processi economici, senza bisogno di giungere alla conduzione a porte chiuse, il Tribunale e le parti si accordano per non mai menzionare il nome del cliente.

Naturalmente, toccherà alla parte denunciante, se possibile ancora prima di avere inoltrato la denuncia, fare presente al magistrato competente questa problematica onde sondare ed esaminare congiuntamente la disponibilità e le possibilità tecniche per assicurare il massimo di protezione all'identità e ai fatti coperti dal segreto bancario, d'affari e commerciale.

L'argomento che spesso viene invocato, specie nel settore terziario, per rinunciare alla presentazione di una denuncia penale è quello della possibile pubblicità negativa conseguente alla rivelazione di un reato di cui si è rimasti vittime.

In effetti, la rivelazione di un reato corrisponde quasi sempre a mettere in luce una lacuna nel proprio sistema di prevenzione e di sicurezza. Ed è anche inevitabile, qualora il procedimento penale giunga fino al processo, che tramite il pubblico dibattimento davanti alla Corte l'opinione pubblica ne sia informata. Questo argomento non è ovviamente privo di una sua validità, dal momento che la fiducia da parte della clientela, esistente e potenziale, costituisce un prezioso capitale per ogni impresa attiva nel settore terziario. Vi sono però da considerare, in un giudizio che ovviamente può farsi soltanto caso per caso, anche questi fatti:

a) quando si tratta di reati d'ufficio, com'è il caso per quasi tutti i reati della criminalità economica ed informatica, l'autorità penale è obbligata ad aprire un procedimento penale non appena ne abbia notizia, anche se la vittima non ha sporto denuncia. Sono conosciuti casi in cui l'autorità penale ha avviato un procedimento e perseguito un reato, anche a parecchi anni di distanza dalla sua esecuzione, di cui ebbe notizia casualmente e da una fonte diversa da quella della vittima e malgrado la vittima avesse deciso di tenere segreto il fatto e, di conseguenza, di non sporgere denuncia.

Questa situazione si è presentata per esempio nel caso di procedimento penale contro un dipendente di banca che ha delinquito presso diverse banche. Poiché in genere l'autorità penale indaga anche sui motivi di cambiamento dei precedenti posti di lavoro, qualche volta si è stabilito che la partenza da un istituto bancario precedente era avvenuta con la dichiarazione di ben servito della banca, malgrado che il motivo della partenza fosse costituito proprio dalla consumazione di reati.

In casi simili, la banca che ha rinunciato alla denuncia sconta presso il pubblico una pubblicità negativa sicuramente maggiore di quella che avrebbe eventualmente scontato se avesse denunciato il reato all'epoca in cui lo aveva scoperto.

b) Trattandosi d'istituti bancari e parabancari sottoposti alla legge federale sulle banche, l'organo di revisione bancaria deve notificare (art. 21 cpv. 3 e cpv. 4 LFBan) alla Commissione federale delle banche le violazioni a prescrizioni di legge constatate all'interno di una banca; la Commissione delle banche a sua volta è tenuta per legge (art. 23-*ter* cpv. 4 LFBan) a notificare all'Autorità penale cantonale i fatti penalmente reprensibili[14].

[14] P. BERNASCONI, *Aspetti penali, amministrativi e di controllo nel mondo finanziario svizzero e ticinese*, in *La piazza finanziaria ticinese*, Lugano, 1984, p. 154 ss.

c) Quantificare le conseguenze pregiudizievoli di una pubblicità negativa è certamente molto delicato. Si conoscono però numerosi casi che hanno coinvolto come vittime di reato economico delle banche, con lo sgradevole ma inevitabile eco di accompagnamento. Non si conoscono però casi in cui quest'eco abbia danneggiato la banca in questione, al punto da cagionare fughe di clienti o simili eventi. Anzi, spesso il processo rappresenta proprio l'occasione di massima pubblicità per rendere note le misure di sicurezza che sono state introdotte per evitare il ripetersi di casi analoghi a quello giudicato nel processo medesimo.

d) Rendere noto pubblicamente che un'impresa bancaria o terziaria denuncia penalmente almeno i casi più gravi permette di ottenere una pubblicità preventiva nei confronti dei potenziali malfattori all'interno o all'esterno della banca.

Infatti, quando sia noto che una banca per principio rinuncia a presentare denuncia penale contro gli autori di reati, questi possono essere indotti a delinquere proprio dalla certezza d'impunità che loro deriva da questo tipo di decisione di principio. Per un dipendente la tentazione di delinquere può infatti essere maggiore sapendo che, in caso di scoperta, al massimo si perde il posto di lavoro, ma che comunque non si deve mai temere il perseguimento penale.

6. La consulenza esterna.

La diffusione dell'informatica nell'impresa richiede un gran numero di specialisti, che non in tutti i settori è facile reperire. Questa scarsità di personale qualificato arrischia talvolta di mettere la sicurezza di un'intera azienda nelle mani dei pochi specialisti in informatica. Pertanto, a maggior ragione appare necessario far capo alla consulenza esterna. I primi consulenti sono evidentemente da trovarsi fra le ditte fornitrici di *hardware* e *software*. Nella scelta di questi fornitori è pertanto importante tenere presente, oltre al fattore dei costi, anche il livello di consulenza specialistica aggiornata che ciascuna è in grado di assicurare.

Anche un ufficio di revisione esterno indipendente — sul modello di quello richiesto alle banche in base all'art. 18 della legge federale sulle banche — rappresenta un valido strumento nel sistema di sicurezza globale dell'azienda. Gli incombe infatti la funzione di verificare l'efficienza dell'organo di controllo interno nella singola azienda, controllando l'allestimento di elenchi di « zone a rischio » dell'azienda, di sistemi di allarme preventivo e di criteri di aggiornamento delle misure di sicurezza interne. Anche in questa scelta, il fattore dei costi non deve fare trascurare il fattore della qualità della consulenza. Raccomanda infatti il criminologo tedesco Ulrich Sieber, la massima autorità europea in questo campo:

« DP internal auditing concerning computer fraud is one of the most advanced and most difficult areas of the DP profession » (*op. cit.*, p. 133).

La medesima raccomandazione può essere formulata anche riguardo alla scelta della compagnia assicuratrice.

Infatti, le compagnie di assicurazione, proprio in virtù della loro funzione, dispongono di un vasto campionario di casi in cui il sistema di sicurezza ha fallito.

Ed è proprio la conoscenza delle esperienze negative che permette l'aggiornamento ed il perfezionamento delle misure esistenti. E sono proprio le esperienze negative, che ogni vittima tende a tenere solo per sé, ad essere quelle più difficilmente accessibili, malgrado siano quelle più istruttive. In quest'ottica appare molto utile disporre di una banca-dati, in cui centralizzare le informazioni raccolte da diversi enti privati riguardo alla casistica. Questi enti ne sarebbero contemporaneamente i fornitori ed i beneficiari, mettendo in comune le rispettive esperienze. Entrano in linea di conto banche, compagnie di assicurazione, società di revisione bancaria, società di certificazione, fiduciari, produttori di *software* e *hardware*, autorità penali ed amministrative, ecc. (cfr. annesso VI).

7. Conclusione.

Infine, non dimentichiamo che il motore di tutti i sistemi economici rimane l'individuo: anche in questo campo, pertanto, la prevenzione deve puntare anzitutto alla motivazione ed alla promozione della responsabilità del singolo collaboratore.

Da un lato, non deve rimanere trascurata l'etica professionale, d'altro lato, il singolo deve essere motivato dimostrandogli che anche il settore della sicurezza ha un suo ruolo, talvolta essenziale, nell'andamento di un'impresa economica. In questo modo si può anche superare la resistenza verso la sicurezza, spesso vissuta come una briglia troppo stretta imposta ai settori « produttivi » dell'azienda. Si può anche superare la diffidenza psicologica da parte dei settori « produttivi » verso i settori « amministrativi », nei quali è inserito anche il reparto addetto alla sicurezza.

Per arginare la diffusione dell'abuso di questo nuovo formidabile alleato che la tecnica ha messa a disposizione dell'economia, è necessario anche l'intervento dei poteri pubblici. Da un lato aggiornando la legislazione, sia amministrativa che penale, ma d'altro lato anche specialmente potenziando e specializzando le autorità incaricate di applicare le nuove leggi. Ma la priorità deve e può rimanere attribuita alla disciplina e prevenzione privata. Questo studio rappresenta un contributo in questa direzione.

ALLEGATO I

CASISTICA GIUDIZIARIA SVIZZERA E STRANIERA.

CASO 1:

Autore: Responsabile del servizio informatico di una media banca di Ginevra.

Metodo: Nel corso di 6 anni, l'autore ha sottratto fondi per Fr. 123'671 complessivamente operando abusivamente su 5 conti detti « senza movimento » e in danno dei conti relativi agli utili di cambio della banca.

L'autore scelse dei conti « senza movimento » poiché i loro titolari non si erano più presentati in banca da molti anni. Questi conti vennero addebitati di determinati importi che furono accreditati a favore di un conto di un terzo sul quale l'autore aveva procura generale come pure a favore di un conto dell'autore medesimo, il quale utilizzò le somme per sue necessità personali.

Egli aveva modificato il programma dell'ordinatore in modo da cancellare ogni volta il saldo reale dei cinque conti abusivamente addebitati, come pure ogni operazione di addebito. Al saldo falso che ne risultava apponeva la data del vecchio saldo.

Reato: *a*) falsità in documenti (art. 251 cod. pen.). Si è stabilito — per la prima volta nella giurisprudenza del Tribunale federale svizzero — che questo reato viene commesso da chiunque introduca dei dati falsi in un ordinatore a scopo d'indebito profitto. Cade infatti sotto la definizione di titolo (art. 110 cod. pen.) anche ogni registrazione o segno la lettura del quale possa avvenire anche soltanto mediante l'utilizzazione di mezzi tecnici, come per esempio mediante lettore di microfilm oppure videoterminale di CED. Basta che il segno o la registrazione incorpori una dichiarazione di origine umana; *b*) appropriazione indebita (art. 140 cod. pen.) questo reato viene commesso anche dal funzionario di banca che è competente esclusivamente per l'esecuzione di mansioni tecniche od amministrative senza compiti di gestione o custodia di beni patrimoniali. Il fatto che il funzionario, bancario o postale, disponga di denaro contante o di crediti è irrilevante. È pure irrilevante se il funzionario dispone o meno del diritto di firmare in nome e per conto della banca oppure sul conto manipolato.

Rif.: Sentenza 18 dicembre 1985 del Tribunale federale (pubbl. in STF 111 IV 119).

CASO 2:

Autore: Procuratore in una grande banca di Zurigo, facente funzione di responsabile del servizio dei conteggi esteri di borsa.

Metodo: Mediante undici manipolazioni abusive, l'autore fece accreditare a favore del suo conto personale circa fr. 90'000 complessivamente. I corrispondenti addebiti vennero effettuati a carico del conto di una filiale americana della banca medesima, simulando altrettante vendite di titoli, che poco tempo dopo l'autore provvedeva ad annullare mediante registrazione abusiva nel CED della banca. Per il controllo di questo tipo di operazioni è richiesta la seconda firma di un altro funzionario di banca. Poiché le operazioni avvengono per *computer*, la seconda firma viene sostituita da un controllo al videoterminale, che consiste nella validazione mediante inserimento del password del secondo funzionario. Il password consiste di sei cifre cambiate periodicamente. L'autore riuscì a scoprire questo password semplicemente rimanendo alle spalle del proprio collega quando questi lo digitava al terminale, potendo quindi leggerlo sul video. L'autore fu così in grado di validare da se stesso le sue operazioni abusive. Queste vennero scoperte perché il programma informatico di controllo prevede una comunicazione automatica in ogni caso in cui risulti una differenza fra i saldi.

Reati: *a*) appropriazione indebita (art. 140 cod. pen.).

L'accusa del reato più grave di truffa venne lasciata cadere poiché presuppone un inganno astuto nei confronti della vittima, ciò che il Tribunale giudicò non essersi verificato nel caso concreto, poiché il *back office* della banca non era tenuto ad effettuare nessun controllo della

documentazione; *b*) falsità in documenti (art. 251 cod. pen.).

È stata considerata documento secondo la definizione penale (art. 110 cod. pen.) la registrazione su nastro magnetico del password facente funzione di seconda firma che l'autore aveva effettuato abusivamente.

Rif.: Sentenza 16 gennaio 1987 dell'Obergericht del Canton Zurigo (NZZ N. 13/1987).

CASO 3:

Autore: Contabile della filiale di una grande banca di Zurigo.

Metodo: *a*) l'autore distrugge copie di ordini di bonifico pervenuti a favore del conto di clienti e le sostituisce con ordini di bonifico a favore di un suo conto, per gli stessi importi, ottenendone l'esecuzione mediante l'inserimento nel *computer* dei dati corrispondenti; *b*) l'autore inserisce nel *computer* un preavviso secondo cui a favore del suo conto era atteso un bonifico di fr. 100'000; successivamente si presentò presso alcune filiali della stessa banca, ottenendo i prelievi poiché i cassieri, interrogando il *computer*, ricevettero risposta positiva riguardo alla copertura esistente sul conto.

Rif.: Sentenza 25 maggio 1981 dell'Obergericht del Canton Zurigo di condanna per truffa, falsità e sottrazione di documenti.

CASO 4:

Autore: Impiegato della filiale cittadina di una banca di in correità con persone all'esterno.

Metodo: Gli autori esterni aprono un conto esibendo un documento d'identità falsificato. L'impiegato della banca allestisce un ordine di accredito per mezzo milione di franchi vistandolo con una firma di fantasia. L'addetta al *computer* registra l'ordine senza verifica della firma apposta sotto il visto per cui il conto venne accreditato della somma. Uno degli autori esterni tentò di prelevare la somma, senza riuscirvi soltanto per il fatto che la firma apposta sulla ricevuta non corrispondeva a quella che figurava sul documento d'identità usato per l'apertura del conto.

Rif.: Polizia cantonale di Zurigo DK NR. 533/1984 (citato da ZIMMERLI E., *Computer-Kriminalitäet*, in *Kriminalistik Mai*, Juli 1987).

CASO 5:

Autori: Due funzionari di una grande banca di Zurigo addetti al controllo nel reparto EED (dopo un corso di tre mesi).

Metodo: Un complice esterno fece piccoli versamenti presso banche all'estero a favore di diversi nominativi presso le filiali di località turistiche svizzere della banca suddetta. Gli ordini di pagamento pervennero per telex alla sede centrale, dove i due controllori li aspettavano, inserendo poi nel *computer* l'ordine per le filiali per un importo moltiplicato per mille. Presso le filiali le somme vennero prelevate in contanti dai complici muniti di falsi passaporti.

Danno: Fr. 620'000 (consumato) e fr. 410'000 (tentato).

Rif.: Sentenza 12 aprile 1976 dell'Obergericht del Canton Zurigo di condanna per truffa e falsità in documenti.

CASO 6:

Autore: Procuratore di una media banca di Lugano addetto al servizio crediti.

Metodo: Dopo avere ottenuto una linea di credito a proprio favore, ha alterato i suoi limiti di competenza per la concessione di crediti, in modo che l'impiegato EED ha accettato la concessione di crediti a favore del funzionario infedele anche quando oltrepassarono il limite di competenza originariamente autorizzato secondo il regolamento interno.

Danno: Circa fr. 50'000 durante un anno.

Rif.: Sentenza 30 aprile 1983 Assise Correzionali Lugano-città di condanna per truffa e falsità in documenti.

CASO 7:

Autore: Capo-operatore presso il Centro di calcolo elettronico del Cantone Ticino.

Metodo: I dati riguardanti le imposte federali e cantonali essendo elaborati secondo un sistema di schede perforate, la procedura d'incasso nei confronti dei contribuenti dipende esclusivamente dall'impianto. Pertanto, l'autore poté conseguire una riduzione nel pagamento delle imposte sia a suo favore che a favore dei suoi creditori. A tale scopo aveva sottratto le schede delle persone interessate evitando l'invio delle diffide di pagamento; inoltre inserì delle schede falsificate per cui il debito fiscale venne estinto.

Danno: Fr. 28'938 in quattro anni.

Rif.: Sentenza 2 ottobre 1970 del Tribunale federale di conferma della condanna per truffa e falsità in documenti (RU 96 1970 IV 85).

CASO 8:

Autore: Contabile di una grande banca di Zurigo addetto ai conteggi di una ditta emittente di carte di credito.

Metodo: l'autore effettuò prelievi indebiti dal suo conto nonché bonifici a favore di conti suoi e di creditori presso altre banche. Per nascondere queste malversazioni appose una codificazione falsa sui documenti giustificativi destinati alla contabilità generale, per cui le ignare impiegate addette alla registrazione elettronica attribuirono tutti gli addebiti al conto interno della banca.

Danno: Circa fr. 450'000 durante due anni.

Rif.: Sentenza 8 novembre 1976 dell'Obergericht del Canton Zurigo di condanna per truffa e falsità in documenti.

CASO 9:

Autori: Una banda internazionale che agiva con la collaborazione di un funzionario di una grande banca di New York addetto al settore dei pagamenti internazionali per via elettronica.

Metodo: Gli autori costituirono una ditta fasulla, a nome della quale spedirono alla banca, da un ufficio nel World Trade Center, un telex con cui ordinavano di bonificare 44 milioni di dollari complessivamente a favore di conti aperti presso due grandi banche di Zurigo ed una grande banca di Losanna. Il funzionario complice, ricevuto il telex fasullo, lo accettò e lo ritrasmise ai destinatari dopo averlo munito della chiave in codice cifrato. Gli autori si presentarono alle banche svizzere per prelevare la somma. Poiché il prelievo era desiderato in contanti, le banche richiesero una mezza giornata per rendere disponibile la somma. Nel frattempo vennero informate dalla Procura pubblica di Lugano, dove erano stati fatti sorvegliare i componenti della banda a causa dei loro movimenti sospetti. Fu così possibile procedere al loro arresto e alla condanna, compreso anche il complice di New York.

Rif.: Sentenza 13 settembre 1979 della Corte delle Assise Criminali di Lugano.

CASO 10:

Autori: Un impiegato della Prudential Bache Securities, succursale di Londra, con un complice all'esterno della ditta.

Metodo: L'autore era addetto al servizio dei titoli europei. Non era però legittimato — e quindi non disponeva del password — ad impartire istruzioni riguardanti transazioni di titoli amministrati presso l'Euroclear Ltd. Presso la sede di Bruxelles di quest'ultima è accentrato il movimento di giro dei titoli del sistema messo in atto dalle banche e dagli agenti di borsa europei allo scopo di evitare lo spostamento fisico dei titoli.

L'autore, in un modo non ancora accertato, riuscì a far pervenire alla Euroclear, mediante canale elettronico, l'istruzione di trasferire Eurobond per un valore di 8,5 milioni di dollari ad una banca di Ginevra. Questo ordine partì il 10 febbraio 1986 e venne eseguito subito, per cui già all'11 febbraio i titoli erano a disposizione a Ginevra, donde vennero trasferiti presso una società finanziaria. Fortunatamente Euroclear segnalò la transazione alla Bache, dove fu possibile accertare che non era autorizzata. Scattato l'allarme, il 12 febbraio l'autorità giudiziaria di Ginevra ordinò il blocco del conto in questione, riuscen-

do a sequestrare la partita di titoli prima che scomparisse.

Secondo un'intervista rilasciata successivamente da un impiegato, un punto debole sarebbe stato costituito dalla possibilità per chi è riuscito a scoprire il password, d'impartire istruzioni dall'esterno degli uffici usando un personal *computer* e collegandosi alla rete telefonica di trasmissione dei dati.

Rif.: Financial Times 2 settembre 1986, Wall Street Journal, 3 settembre 1986, p. 11.

CASO 11:

Autori: responsabili del settore divise della Herstatt Bank di Colonia (posta in liquidazione forzata nel 1974 con un saldo passivo di 1,2 milioni di marchi).

Metodo: A causa di numerose speculazioni avventate sul mercato delle divise gli autori cagionarono enormi perdite alla banca.

Riuscirono ad occultarle manipolando la consolle di un piccolo *computer* attraverso il quale tutti i dati riguardanti il settore delle divise dovevano pervenire al computer centrale della banca. A questo scopo bastava schiacciare il tasto « interruzione » (Abbruchtaste) in modo che la singola transazione non veniva trasmessa al *computer* centrale, pur ottenendo una regolare registrazione per il contraente.

Per parecchio tempo fu quindi possibile mantenere più basso del reale il volume complessivo delle transazioni e, quindi, anche quello delle perdite che ne erano conseguite.

Gli autori dovettero superare una misura di sicurezza prevista appunto contro l'abuso dell'uso del tasto « interruzione ». Infatti quando veniva azionato questo tasto, sul conteggio stampato dal *computer* veniva impressa automaticamente la menzione « interruzione ». Poiché questa menzione avrebbe portato alla scoperta delle manipolazioni abusive, gli autori toglievano il formulario del conteggio non appena era stato stampato ma ancora prima che fosse impressa la menzione « interruzione », che pertanto andava a finire sul rullo vuoto.

Rif.: Sentenza 16 febbraio 1984 del Tribunale di Colonia.

CASO 12:

Autori: Il responsabile ed il personale di una compagnia di assicurazione, la Equity-Funding-Corporation, fra cui anche i tre addetti al Centro EED della stessa.

Metodo: La Equity vendeva ad una compagnia di riassicurazioni contratti fittizi di assicurazione sulla vita. Nel periodo dal 1970 al 1972 ne vendette circa 56'000 per un valore complessivo di oltre 30 milioni di dollari. La compagnia acquirente poté essere ingannata poiché riguardo all'esistenza dei contratti non richiedeva alcuna prova documentale, limitandosi ad accettare la comunicazione fornitagli elettronicamente dalla Equity. La sua fiducia venne mantenuta per il fatto che la Equity forniva per ogni contratto tutte le indicazioni usuali, sia anagrafiche, che sanitarie ed assicurative. Se questi dati avessero dovuto essere elaborati manualmente o meccanicamente, non sarebbe stato materialmente possibile preparare così tanti contratti fasulli.

La Equity preparò un programma per il proprio Centro EED grazie al quale venivano « prodotti » nuovi contratti facendo apportare alcune modifiche ai contratti preesistenti: venivano cambiati i numeri progressivi dei contratti, mentre l'importo del premio e della copertura assicurativa venne mutato facendolo moltiplicare per il fattore 1,8. Grazie ad altri programmi informatici tutti questi dati fittizi fluivano anche nel bilancio della Equity contribuendo al rialzo delle sue azioni.

Rif.: Sieber Ulrich, Computerkriminalitäet und Strafrecht, Köeln, 1980, p. 1437.

CASO 13:

Autori: Due impiegati di una grande banca svizzera addetti come operatori al CED.

Metodo: Un funzionario della Dogana francese offrì ai due operatori il pagamento in denaro di informazioni provenienti dalla banca in cui lavoravano. Attraverso un intermediario vennero pattuiti FF 500'000 in pagamento di nastri magnetici con la registrazione di programmi. Si trattava, in particolare,

dell'adattamento dell'intero sistema informatico della banca medesima. Vennero consegnati cinque nastri che furono affidati alla Scuola superiore d'informatica dell'Esercito a Rennes per essere decodificati.

I nastri però non risultarono contenere dati personali di clienti. Secondo la banca derubata il loro contenuto non poté comunque essere di utilità per la Dogana francese, anche in considerazione del numero esiguo di nastri finiti nelle sue mani per rapporto al numero totale di nastri — circa 6.000 — contenuti nel CED della banca.

I due autori vennero condannati a pene detentive di 4 e di 3 anni per titolo di furto, spionaggio economico e violazione del segreto bancario.

Rif.: Sentenza del Tribunale penale di Losanna dell'11 luglio 1984. Nella sentenza con cui il Tribunale federale ha confermato la suddetta decisione cantonale di condanna si precisa in particolare quanto segue: *a*) furto (art. 137 cod. pen.). Un nastro magnetico sul quale è stato registrato un programma di sviluppo di una banca può costituire oggetto di un furto.

L'indebito arricchimento da parte dell'autore non deve essere calcolato soltanto in base al valore intrinseco dell'oggetto, bensì anche in base al valore connesso alla sua utilizzazione; *b*) spionaggio economico (art. 273 cod. pen.). Permettendo l'accesso a doganieri stranieri ai programmi informatici di una grande banca svizzera, gli autori hanno messo in pericolo non soltanto il segreto d'affari della banca stessa bensì anche, in larga misura, gli interessi economici della Svizzera (cfr. STF 108 IV 47); *c*) violazione del segreto bancario (art. 47 della legge federale sulle banche). Il terzo estraneo ad una banca che tenta di ottenere dati coperti dal segreto bancario, non può essere considerato autore bensì soltanto complice di violazione del segreto bancario. Può essere punibile anche se l'autore, ossia il funzionario di banca, si è limitato ad un tentativo di violazione del segreto bancario.

(Cfr. sentenza pubblicata in STF 111 IV 74 ss.).

Caso 14:

Autori: Diversi componenti di una banda internazionale finora non identificati.

Metodo: Il giorno precedente un fine settimana prolungato (venerdì di Pentecoste) vennero prelevati circa 250.000 franchi svizzeri dai distributori automatici di banconote del sistema bancario svizzero (Bancomat).

I prelievi avvennero contemporaneamente in diverse località svizzere, utilizzando 250 carte plastificate false. Grazie alla connivenza o alla grave negligenza di cinque titolari di carte, fu possibile conoscere il numero di codice di ciascuno, che altrimenti non è leggibile dalla carta stessa. Di ogni carta vennero prodotti 50 esemplari falsi. Poiché il sistema svizzero è ancora privo del collegamento *on line*, i prelievi vennero utilizzati, ma soltanto a concorrenza del limite massimo previsto per ogni giorno, ossia 1.000 franchi. Pertanto, quando le carte false vennero inserite per tentare un secondo prelievo, vennero ingoiate dagli apparecchi, poiché l'utilizzazione oltre il limite massimo era stata memorizzata nella banda magnetica.

Fu così possibile bloccare ulteriori prelievi e risalire agli autori. Sono ipotizzabili i reati di furto (art. 137 CPS) e di falsità di documenti (art. 251 CPS) ma non quello di truffa (art. 148 CPS).

Fonte: Autorità giudiziaria di Bellinzona (episodio del 20 maggio 1988).

Caso 15:

Autori: Due persone di cui una avente funzione di controllare presso la Prudential Bache Securities Inc. in Londra.

Metodo: Il controllore riuscì a far trasferire dalla Pru-Bache titoli per 8,5 milioni di dollari di valore, inserendosi nel sistema informatico di trasferimento mediante un modern ed utilizzando un home computer.

Essendosi impadronito del codice, l'accredito venne eseguito, a favore di un conto aperto presso una società finanziaria a Ginevra. Poiché le operazioni riguardanti il trasferimento internazionale di titoli sono centralizzate presso l'Euroclear a Bruxelles, quest'ultima ne diede conferma alla Pru-Bache, che riu-

scì ad ottenere dall'autorità giudiziaria di Ginevra il blocco dei titoli sottratti, prima che gli autori potessero disporne.

Rif.: The Wall Street Journal 3 settembre 1986.

CASO 16:

Autori: I membri di una banda internazionale (ancora in via di identificazione).

Metodo: Gli autori, agendo presso la filiale di Londra della Unione di Banche Svizzere, hanno compiuto manipolazioni che permisero loro di superare le barriere interne di accesso in modo da accreditare abusivamente una somma di 82 milioni di franchi. I sistemi di controllo permisero di scoprire l'abuso in tempo per bloccare le operazioni ed informare la banca di Nyon presso Losanna, presso cui si trovava il conto beneficiario.

Le due persone che si presentarono per effettuare il prelievo vennero così arrestate.

Rif.: Tages Anzeiger 6 luglio 1988.

NOTA COMPLEMENTARE:

Nel corso degli ultimi anni la stampa svizzera e francese ha riferito a più riprese di episodi simili grazie ai quali le autorità doganali francesi sarebbero riuscite ad entrare in possesso d'informazioni riguardanti clienti francesi di banche svizzere. Sembra però che si sia trattato di modi tradizionali per entrare in possesso di questi dati, senza che vi sia mai stato un accesso diretto oppure indiretto a CED bancari. L'argomento è comunque stato evocato nel corso d'incontri a livello governativo fra i due Paesi durante il 1984. Si veda comunque sul tema: *a*) arresto di due doganieri a Basilea, nel 1980, mentre trattavano per ottenere informazioni coperte dal segreto bancario. (Wirtschaftswoche N. 43/21 ottobre 1983); *b*) presentazione di denunce penali contro funzionari doganali francesi (risposta del Consiglio federale all'interpellanza del consigliere nazionale Couchepin del 13 febbraio 1983); *c*) rivelazioni riguardanti nuovi tentativi in danno di banche di Ginevra (conferenza stampa 9 marzo 1984 di un direttore di banca a Ginevra); *d*) nuova lista di 700 clienti di banche svizzere pervenuta alle autorità francesi, presumibilmente tramite una società investitrice olandese (dichiarazioni alla trasmissione televisiva francese « Droit de reponse » del 5 ottobre 1985 e Tribune de Genève 22 ottobre 1985, p. 3).

II. Norme penali vigenti.

COMPUTER CRIMES
reati già punibili in base al
Codice Penale Svizzero vigente (cod. pen.)

FURTO/SPIONAGGIO

- copiatura e sottrazione di supporti di dati (dischetti, nastri, stampati, ecc.)
  (art. 137 cod. pen. furto; art. 140 cod. pen. appr. indebita; art. 159 cod. pen. amm. infedele; art. 254 soppressione di documenti)
- sottrazione d'impianti EED (in tutto o in parti staccate)
  (cfr. i reati suddetti)
- sottrazione d'informazioni (dati, programmi, ecc.) (viol. del segreto d'affari art. 162 CPS oppure bancario art. 47 Legge federale sulle Banche, spionaggio economico art. 273 cod. pen.) art. 13 lett. f e g della Legge federale sulla concorrenza sleale

FURTO DI TEMPO

- vendita a terzi non autorizzata di tempo d'uso del CED
- utilizzazione da parte di terzi di programmi mediante « Datenleitung »
- utilizzazione non autoriz. del tempo del CED da parte di addetti per propri fini (art. 159 amministrazione infedele)

DANNEGGIAMENTO

- danni intenzionali o colposi arrecati ad impianti EED
- mediante intervento esterno (art. 145 cod. pen. danneggiamento; art. 221, 222 cod. pen. incendio; art. 223 cod. pen. esplosione, ecc.)
- mediante intervento interno sul funzionamento (art. 145 cod. pen. danneggiamento)

TRUFFA

- abuso d'impianto EED per ottenere prestazioni indebite (art. 148 cod. pen. truffa)
- modifica di dati di input
- modifica di dati registrati
- abusi nell'operating

FALSIFICAZIONE

- alterazione/abuso di scritti prodotti mediante EED (art. 251 cod. pen. falsità in documenti)

III. Norme penali proposte.

NUOVI COMPUTER CRIMES
reati punibili in base all'avamprogetto
di revisione del Codice Penale Svizzero (ACP)

TRUFFA

- truffa mediante EED (art. 147 ACP)
- truffa mediante carte d'assegni o di credito (art. 148 ACP)

FURTO

- sottrazione di una prestazione fornita mediante EED (art. 150 cpv. 4 ACP cosid. Zeitdiebstahl)

FURTO/SPIONAGGIO

- acquisizione illecita di dati o programmi (art. 143 ACP, cosid. Softwarendiebstahl)

DANNEGGIAMENTO

- modifica/cancellazione di dati o programmi mediante influsso diretto o indiretto su EED (art. 144 cpv. 2 ACP)

FALSIFICAZIONE

- allestimento/abuso di uno scritto apparentemente risultato da un impianto EED (art. 251 n. 1 cpv. 4 ACP per i privati) (art. 317 n. 1 cpv. 4 ACP per i funzionari)
- falsificazione/abuso di contabilità registrata su impianto EED (art. 251-*bis* cpv. 2 ACP)

IV. I REATI INFORMATICI NEL CODICE PENALE SVIZZERO IN BASE ALL'AVAMPROGETTO DI REVISIONE DEL 14 AGOSTO 1985.

ART. 143 (nuovo).

(*Acquisizione illecita di dati*).

1. Chiunque, per procacciare a sé o ad altri un indebito profitto, si procura illecitamente dati o programmi registrati elettronicamente, è punito con la reclusione sino a cinque anni o con la detenzione.

2. Se il colpevole ha agito senza voler trarne profitto, è punito, a querela di parte, con la detenzione o con la multa.

ART. 144 cpv. 1 e 3 (attualmente art. 145).

(*Danneggiamento*).

1. Chiunque deteriora, distrugge o rende inservibile una cosa altrui, o su cui grava un diritto d'uso o d'usufrutto a favore di altri, è punito, a querela di parte, con la detenzione o con la multa.

2. È punito con la stessa pena, a querela di parte, chiunque, senza autorizzazione, modifica o cancella dati o programmi registrati elettronicamente.

3. (attuale cpv. 1-*bis*).

4. Il giudice può pronunciare la reclusione sino a cinque anni se il delinquente ha causato un danno considerevole. Il perseguimento ha lungo d'ufficio.

ART. 147 (nuovo).

(*Abuso di un impianto per l'elaborazione di dati*).

Chiunque, per procacciare a sé o ad altri un indebito profitto, provoca un processo d'elaborazione o di trasmissione di dati il cui risultato è inesatto, oppure ostacola un tale processo il cui risultato sarebbe stato esatto, causando in tal modo un trasferimento d'attivi a scapito di un terzo, è punito con la reclusione sino a dieci anni o con la detenzione.

ART. 148 (nuovo).

(*Abuso di carte d'assegni o di credito*).

Chiunque, nonostante la sua insolvenza, usa una carta di garanzia per assegni, una carta di credito o un analogo mezzo di pagamento obbligando in tal modo l'emittente ad effettuare un pagamento ad un terzo, è punito con la detenzione sino a cinque anni.

ART. 150 (attualmente art. 151).

(*Scrocco di una prestazione*).

Chiunque, senza pagare, ottiene una prestazione sapendo che la stessa è data soltanto a pagamento, in modo particolare l'utilizzazione di un mezzo di trasporto pubblico,

l'accesso ad una rappresentazione, ad un'esposizione o ad una manifestazione simile,

una prestazione fornita da un impianto di elaborazione dei dati o il funzionamento di un apparecchio automatico,

è punito, a querela di parte, con la detenzione o con la multa.

ART. 251.

(*Falsità in documenti*).

1. Chiunque, a scopo d'inganno nei rapporti giuridici,

forma un documento falso, altera un documento vero oppure abusa dell'altrui firma o segno a mano per formare un documento supposititzio,

forma uno scritto d'interesse giuridico che dà l'impressione d'essere il risultato di un processo automatico d'elaborazione di dati,

o fa uso di un tale documento o di un tale scritto,

è punito con la reclusione sino a cinque anni o con la detenzione.

(L'attuale n. 2 è stralciato e l'attuale n. 3 diventa il nuovo n. 2).

ART. 251-*bis* (nuovo).

(*Falsa contabilità*).

1. Chiunque, a scopo d'inganno nei rapporti giuridici e in violazione di un obbligo prescritto dal diritto commerciale, tiene una falsa contabilità, in particolare effettua un'iscrizione falsa, allestisce in modo inesatto un inventario, conti di esercizio o un bilancio, è punito con la reclusione sino a cinque anni o con la detenzione.

2. La registrazione su supporti di dati o immagini è assimilata ad uno scritto.

3. La stessa pena si applica a chi fa uso di un tale documento o di una tale

registrazione a scopo d'inganno nei rapporti giuridici.

ART. 317.

(*Falsità*).

1. I membri di un'autorità, i funzionari e i pubblici ufficiali che, a scopo d'inganno nei rapporti giuridici,

formano un atto falso o alterano un atto vero,

abusano dell'altrui firma o segno a mano per formare un atto suppostizio,

formano uno scritto d'interesse giuridico che dà l'impressione di essere il risultato di un procedimento automatico di elaborazione di dati,

attestano in modo contrario alla verità in un documento un fatto avente portata giuridica, in particolare autenticano una firma o un segno a mano falsi o una copia non conforme all'originale,

sono puniti con la reclusione sino a cinque anni o con la detenzione.

2. Se il colpevole ha agito per negligenza, è punito con la detenzione sino a sei mesi o con la multa.

V. BIBLIOGRAFIA.

A) LETTERATURA STRANIERA:

AMERICAN BAR ASSOCIATION,
Report on Computer Crime, New York, 1983.

ASSOCIAZIONE ITALIANA EDP AUDITORS,
La frode EDP nelle banche e nelle assicurazioni, in *Controllo dei sistemi EDP*, Milano, febbraio 1985.

BEQUAI August,
How to prevent Computer Crime, New York, 1983.

BIASIOTTI Adalberto e AA.VV.,
Computer Crime. Una concreta strategia di difesa, Atti del Convegno di Roma 30 aprile 1985 della Ross Collins (Italia) S.p.A.

BRANDT Allen,
Die grössten Computer-Betrugsfälle in Der Schweizer Treuhänder 2/1978, p. 2 ss.

CASTELLI Gian Maria,
Il dolo informatico. Come combattere il computer crime, Milano, 1986.

CHAMOUX Françoise e J.-P.,
Adaptation du droit à la vulnérabilité informatique en Europe, in *Securicom*, 1984, Parigi, 1984, Ed. SEDEP.

ID.,
Menaces sur l'ordinateur, Parigi, 1986.

CORRERA Michele-MARTUCCI Pierpaolo,
I reati commessi con l'uso del computer, Milano, 1987.

GEMIGNANI Michael,
Computer Law, New York, 1985.

GROPP Walter,
Die Codekarte: der Schlüssel zum Diebstahl, in *Juristen-Zeitung, 1983, p. 487 ss.*

MANDELL Steven,
Computer Data Processing and the Law, New York, 1984.

JEANDIDIER Wilfried,
Les truquages et usages frauduleux de cartes magnétiques, La Semaine Juridique L, Doctrine, 1986, 3229.

NIMMER Raymond,
The Law of Computer Technology, Boston, 1985.

OCSE,
Computer related crime: Analysis of Legal Policy, Paris, 1986.

PARKER Donn-NYCOM-OÜRA,
Computer Abuse, 1973 Ed. Standford Institute Menlo Park California aggiornamento 13 aprile 1979, in *National Criminal Justice Information and Statistic Service*, Washington D.C., 1979.

PARKER Donn,
Fighting Computer Crime, New York, 1983.

PESCATORE Claude,
Kriminalität in Zusammenhang mit elektronischem Geld, Luxemburg, 1986.

SARZANA Carlo,
Sviluppo tecnologico e criminalità, in *Informatica ed evoluzione giuridica nell'attività economica*, p. 159 ss. Atti del Seminario ISTIFID, 18-19 ottobre 1984, Roma.

SIEBER Ulrich,
Informationstechnologie und Strafrechtsreform, Köln, 1985.

ID.,
Computerkriminalität und Strafrecht, Köln, 1980.

ID.,
International Handbook on Computer Crime, New York, 1986.

UNITED NATIONS
United Nations Commission on International Trade Law (Uncitral) Draft Legal Guide on Electronic Funds Transfers, Report of the Secretary-General, A/CN 9/250 Add. 4/19 aprile 1984, Chapter on Fraud, Errors, Improper Handling of Transfer Instruction and Related Liability.

B) LETTERATURA SVIZZERA:
(testi riferiti al diritto e alla pratica svizzeri)

AA.VV.,
Sécurité et informatique, Atti del Simposio organizzato a Ginevra/Losanna 11-12 maggio 1982, in *Fides Mitteilungen*, 3/82.

BAUKNECHT Kurt,
Computerkriminalität in Wirtschafts kriminalität, Zurigo, 1982, Ed. Neutra AG.

BERNASCONI Paolo,
Habeas Data - Guardie e ladri computerizzati, in *Almanacco Ticinese Bellinzona, 1983, p. 58 ss.*

ID.,
L'abuso del computer nella criminalità economica, Atti del convegno CEDA, 14 novembre 1985, Lugano, p. 95 ss.

BERNASCONI Paolo,
Preventionsmassnahmen gegen grenzüberschreitende Wirtschaftskriminalität, in Atti World Economic Forum, Davos, 1987.

BRETSCHER Max F.,
Revisionsprobleme bei Mini-und Mikrocomputer, in *Fides Mitteilungen*, N. 39/83, Zurigo.

ID.,
EDV-Kriminalität: gibt es sie überhaupt?, in *Der Schweizer Treuhänder*, Zurigo, Novembre 1985.

FISCHER Thomas,
Computerkriminalität, Gefahren und Abwehrmassnahmen, Berna, 1979, Betriebswirtschaftliche Mitteilungen, Heft 71.

INSTITUT D'ECONOMIE BANCAIRE de l'Université de St. Gall,
Révision du traitement électronique des informations dans les établissements de crédit, in *Collection de révision bancaire*, vol. 4/1980.

ROHNER Louis,
Computerkriminalität, straf. Probleme bei Zeitdiebstahl und Manipulationen, in *Computer und Recht*, Vol. I, Zurigo, 1976.

ROTH Robert,
La délinquance informatique saisie par le droit pénal, in *Semaine Judiciaire*, 109 (1987), 97 ss.

SCHMID Niklaus,
Missbräuche in modernen Zahlungs- und Kreditverkehr, Berna, 1982.

ID.,
Zur Computerkriminalität, in *Banken zwischen Legalität und Kriminalität*, Heidelberg, 1980, p. 145 ss.

ID.,
Zur strafrechtlichen Erfassung von Missbräuchen im Bereiche des bargeldlosen, insbesondere elektronisch abgewickelten Zahlungs- und Kreditverkehrs, in *Revue Pénale Suisse*, 104, 1987, 129.

STAUDER Bernd,
Les nouveaux moyens électroniques de paiement, Lausanne, 1987.

STEINER Albert,
EDV-Sicherheit bei der Bank, in *Schweizer Bank*, 88/4, p. 38 ss.

STRATENWERTH Günter,
Computerbetrug in Zeitschrift für Strafrecht, Bd. 98 (1981), p. 229 ss.

ZIMMERLI Erwin, LIEBI K.,
Computermissbrauch-Computersicherheit, Ingelheim/Küsnacht, 1984.

ID.,
Computer-Kriminalität. Tat. Täter Aufdeckung, in *Kriminalistik*, maggio-luglio 1987.

ZWEIFEL Sibylle,
Buchführungsdelikte mittels EDV und Massnahmen zu deren Verhinderung, Zürich, 1984.

VI. La banca dati della criminalità informatica