

## CRIMINALITÀ E TECNOLOGIA: IL CASO DEI « COMPUTER-CRIMES »

CARLO SARZANA (\*)

SOMMARIO: 1. - Il computer come chiave di volta della nuova società industriale. — 2. - La « cashless society ». L'Electronic Funds Transfer System (EFTS). — 3. - Criminalità economica e « new white collar crimes ». Il costo del « computer-crime ». — 4. - Definizione e tipologia dei « computer-crimes ». — 5. - Fasi dell'EDP e modalità di commissione dei « computer-crimes ». — 6. - Il caso della Equity Funding Corporation of America. — 7. - Il profilo psicologico del « computer-criminal ». — 8. - La pericolosità dei « computer-crimes ». Facilità di commissione e difficoltà di scoperta. — 9. - Le difficoltà di perseguimento dei « computer criminals ». — 10. - I problemi tecnici della prevenzione dei « computer-crimes ». — 11. - Prospettive future nello sviluppo dei « computer-crimes ». — 12. - Conclusioni.

1. — Ritengono gli scienziati che fra le rivoluzioni del ventesimo secolo, la più grande, la prima senza ombra di dubbio, sia quella determinata dal computer: essa supera la stessa energia atomica e la corsa spaziale.

È l'espressione del calcolo, della memoria e del giudizio, una nuova dimensione e volontà del pensiero (1).

In particolare il computer ha determinato una condizione di vita economica totalmente nuova giacché ha creato un nuovo ambiente tecnologico nel mondo degli affari consentendo nuovi modelli di elaborazione e di gestione dei dati e con ciò assumendo una funzione decisiva nel mondo economico moderno. Il computer, cioè, è venuto ad assumere un ruolo coadiuvante (ed in certe condizioni decisivo) nella *leadership* dell'impresa come strumento di scelta decisionale. Esso in definitiva può considerarsi il simbolo riassuntivo della nuova fase di processo tecnologico apertasi nella società industriale (2).

---

(\*) Direttore dell'Ufficio Studi e Ricerche della Direzione Generale per gli Istituti di Prevenzione e Pena.

(1) L'affermazione è di VIKTOR MICHAILOVIC GLUKOV, direttore dell'Istituto di Cibernetica a Kiev, ed è riportata da V. FROSINI nel volume *Cibernetica, diritto e società*, Milano, 1973, p. 71.

(2) FROSINI, *op. cit.* alla nota 1), p. 72. Sulla storia e sul funzionamento del computer, vedi BORRUSO, *Civiltà del Computer*, Roma, 1978.

L'espansione del numero dei computers, oltre che dei settori di impiego, è stata enorme almeno negli Stati Uniti: si è passati dai 45.000 computers circa dell'anno 1967 a 150.000 circa della fine dell'anno 1976, con una previsione di circa 500.000 per gli anni '80 (3).

Stime approssimative per l'Europa occidentale parlano di circa un centinaio di migliaia di computers attualmente in funzione e le installazioni sono in continuo aumento. Esso è ormai alla base dell'industria moderna così come dell'apparato militare e burocratico onde giustamente è stato definito: « *the workhorse of modern society* ».

In continuo aumento è anche il numero del personale impiegato nel settore dei computers. Nel 1975 lo Stanford Institute ha accertato che negli Stati Uniti circa 2.230.000 persone lavoravano direttamente con i computers, il che rappresentava il 3% della forza lavorativa totale statunitense (circa 81.000.000 di persone) (4).

La tecnologia del computer si è sviluppata in modo tale da superare la comprensione dell'uomo medio. Basti pensare che il computer IBM-370 ha una capacità di memorizzazione settemila volte superiore a quella dell'UNIVAC 1, il primo computer commerciale (5), una velocità molto maggiore ed una enorme capacità di « storage » dei dati.

L'avvento dell'era del computer è stato seguito da una aumentata automazione della contabilità e della registrazione di operazioni finanziarie e commerciali. Il trattamento elettronico dei dati è essenzialmente usato dalle imprese per le grandi operazioni di « routine » riguardanti in particolare i bilanci, il pagamento di fatture, gli inventari, ecc...

In definitiva si può affermare che, almeno negli Stati Uniti, il sistema economico dipende quasi totalmente dall'EDP (Electronic Data Processing): invero più dell'80% degli affari dipendono, in un modo o nell'altro, dai computers.

---

(3) PARKER, *Crime By Computer*, New York 1976, p. 295. Secondo BEQUAI all'ottobre del 1978 erano in funzione negli Stati Uniti circa 190.000 computers dei quali 10.000 circa appartenenti al Governo Federale, 80.000 all'industria privata e 100.000 minicomputers (« *Organized Crime in the Computer Arena* », in *The Police Chief*, 1978, p. 24).

(4) PARKER, *op. cit.* alla nota 3), p. 295.

(5) BEQUAI, *White-Collar Crime*, Lexington, Massachusetts, 1978, p. 107.

La paralisi di 100 « *Key-computer* » potrebbe facilmente, secondo alcuni esperti, distruggere l'economia di molti Stati dell'Unione (6).

2. — Bisogna ora tenere presente che ci avviamo in un futuro molto prossimo a quella che è stata definita la « *Cashless-Society* », cioè ad una società senza contanti, basata su un sistema computerizzato di pagamenti e transazioni denominato « *Electronic Funds Transfer System* », (EFTS: Sistema Elettronico per il Trasferimento di Fondi).

Il sistema può implicare il trasferimento di fondi dal conto dell'acquirente a quello del venditore, da quello del datore di lavoro a quello dell'impiegato ovvero operazioni finanziarie tra due o più Istituti bancari, siano essi nazionali od esteri. Il Congresso degli Stati Uniti ha nominato nel 1974 una Commissione per lo studio del EFTS la quale ha iniziato i suoi lavori nel 1976.

Tuttavia già esistono negli USA sistemi parziali di EFTS. Il primo, inaugurato nel 1970, è denominato *Automated Clearing Houses* (ACHs; stanze di compensazione automatizzate) ed è in funzione in molte aree della *West Coast*. I dati necessari sono registrati su bande magnetiche ed il computer è adoperato per trasferire le informazioni e i dati necessari al pagamento nell'ambito degli Enti partecipanti al sistema (società, istituti bancari, ecc.).

L'ACHs è adoperato per il pagamento di stipendi, di dividendi, accreditamenti vari, ecc. in sostituzione degli chèques (7).

Per quanto riguarda in particolare il pagamento degli stipendi, il sistema funziona approssimativamente nel modo seguente. Lo stipendio di un impiegato viene codificato su bande magnetiche o schede perforate consegnate ad una locale Federal Reserve o ad una sua succursale. In seguito la banca del datore di lavoro effettua il pagamento a quella dell'impiegato per mezzo di una cessione interbancaria con la Federal Bank.

Tutte le informazioni riguardanti il trasferimento dei fondi sono registrate su bande magnetiche o su schede perforate (8).

Un altro sistema già in funzione in diversi Stati dell'Unione è quello denominato *Point-of-Sale System*: (POSS: Sistema dei

---

(6) BEQUAI, *Computer Crime: a growing and serious problem*, in *Police Law Quarterly*, 1976, 6/1, p. 24.

(7) BEQUAI, *op. cit.* alla nota 5), p. 187.

(8) BEQUAI, *op. cit.* alla nota 5), p. 164-165.

Punti di Vendita). Il sistema raggruppa una o più banche, uno o più negozi ed i clienti delle banche medesime. Un terminale è installato presso ciascuno dei negozi collegati ed i clienti, al momento degli acquisti, consegnano all'impiegato addetto i loro tesserini di identificazione. Questi ultimi vengono inseriti nel terminale collegato al computer della Banca ed il sistema accredita la somma dal conto dell'acquirente a quello del venditore (9).

In prosieguo di esposizione sarà fatto cenno del rapporto tra EFTS e sviluppo della nuova forma di *white-collar crimes*.

3. — Lo sviluppo di siffatta tecnologia è stato accompagnato dal sorgere di una nuova forma di criminalità *white-collar* denominata *computer-crime* e di cui sarà data in seguito la definizione ed illustrata la tipologia.

Il *computer-crime* è uno dei tipi di delitti che rientra nel campo di indagine della speciale branca della criminologia detta economica. Esso è infatti anche un crimine economico, inteso il termine in tema ampio, in quanto trattasi di un atto illecito il quale colpisce in modo primario gli interessi individuali, abusando degli strumenti della vita economica e conseguentemente danneggiando anche gli interessi economici della collettività (10).

Dal punto di vista teorico, il *computer-crime* rientra, almeno nelle sue forme più frequenti, negli *occupational-crimes* in quanto commesso in prevalenza da impiegati contro datori di lavoro (11), o anche negli *special opportunity crimes*, in quanto per la sua commissione l'autore si avvale, appunto, di una speciale opportunità creata o altamente intensificata dalle attuali molto complesse funzioni ed organizzazione dei sistemi tecnologici ed economici (12) (13).

(9) BEQUAI, *Computer Crime*, Lexington, Massachusetts, 1978, p. 187. Vedi anche *op. cit.* alla nota 5), p. 165.

(10) TIEDEMANN, *The international situation of research and legal reform work in the field of economic and business crime*, in *Ann. Intern. Criminologie*, 1978, Vol. 17, p. 61.

Sulla criminalità economica in genere, vedi l'esauriente studio di DI GENNARO-VETERE, *La criminalità economica*, in *Quad. Crimin. Clinica*, 1977, pag. 503.

(11) CLINARD-QUENNEY, *Criminal Behavior System: A Typology*, citato nello studio di DI GENNARO-VETERE di cui alla nota 10).

(12) HOROSZSKY, *White Collar Crime: Special Opportunity Crime*, cit. nello studio di DI GENNARO-VETERE.

(13) Dall'indagine eseguita da PARKER è risultato che gli autori di 293 casi di «*computer-abuse*», accertati sino a tutto il dicembre 1974, appartenevano in

Sul piano criminologico, lo studio dei *computer-crimes* presenta i problemi classici delle indagini sui crimini *white-collar*, sia pure con qualche particolarità di rilievo.

Anzitutto vi è il problema del *dark number*. I casi accertati da PARKER negli Stati Uniti sino al 1975 ammontavano a 374, ma lo stesso Autore ha accertato che *computer-crimes* erano stati commessi in numerosi altri Stati e cioè, in Belgio, Brasile, Canada, Corea, Danimarca, Francia, Germania Occidentale, Giappone, Jugoslavia, Olanda, Norvegia, Regno Unito, Sud Africa e Svezia (14).

Secondo WALLACE S. BRUSCHWEILER, direttore della divisione internazionale della *Data Security Holding*, una Società specializzata nell'accertare e prevenire questo tipo di crimini, dal 1958 alla fine del 1978 la società ha verificato in tutto il mondo occidentale 636 casi di truffe e reati commessi per mezzo del computer (15).

Anche in Italia si è giunti alla realizzazione dei *computer-crimes*. In una Banca di Milano, infatti, si è scoperto recentemente che alcuni impiegati addetti al servizio elaborazione dati avevano dirottato sui propri conti cifre considerevoli stornandole da quelli dei principali clienti della Banca stessa (15 bis).

Si ha ragione di credere, però, che i casi non accertati o non denunciati rappresentino una percentuale altissima. Stime prudenziali valutano all'85% la percentuale di tali casi, mentre altre stime parlano di un rapporto di uno a cento (16). I settori più colpiti, secondo i risultati delle indagini di PARKER, erano stati, all'ottobre 1973, i seguenti: Banche, n. 70 casi pari al 19% del totale; Istruzione, 68 casi pari al 18%; Enti governativi, n. 61 casi pari al 16%; Industrie manifatturiere, n. 46 casi pari al 12%; Assicurazioni, n. 18 casi pari all'8%; Compu-

---

prevalenza al settore dell'EDP (n. 125 casi) oppure a quello dirigenziale o amministrativo delle varie Società interessate (n. 31 casi).

Su un totale di 482 persone coinvolte nei casi sopraindicati di «*computer-abuse*», ben 269 appartenevano al settore dell'EDP mentre 33 appartenevano al settore dirigenziale o amministrativo. (*op. cit.* alla nota 3), p. 53).

(14) *Op. cit.* alla nota 3), p. 37.

(15) MODULO, *È meglio il computer che il grimaldello*, in *L'Espresso*, gennaio 1979.

(15 bis) MODULO, *op. cit.* alla nota 15).

(16) La prima stima è indicata da PARKER, *op. cit.* alla nota 3), pag. 27. La seconda è incidentalmente riportata in *The Cost of Crimes Against Business*, U. S. Department of Commerce, Washington, January 1976, p. VI.

ter-Services, n. 14 casi pari al 6%; Trasporti, n. 9 pari al 2% (17).

Il numero dei *computer-crimes* accertati può sembrare trascurabile rispetto a quello dei crimini tradizionali ma occorre considerare che le perdite dovute ai crimini in oggetto sono altissime ove rapportate a quelle derivanti dalle frodi e dalle appropriazioni indebite tradizionali. È stato infatti stimato che la perdita media risultante dalle appropriazioni indebite commesse *by computer* è 10 volte più alta della perdita media di 100.000 dollari derivante dalle appropriazioni indebite tradizionali (18). Recenti ricerche eseguite dallo Stanford Research Institute hanno, in particolare, accertato che in 64 casi di *white collar crimes* compiuti nel 1970 e non collegati all'uso del computer la perdita media era stata di 100.000 dollari, mentre nello stesso periodo, in 12 casi di *computer-crimes*, la perdita media era stata di 1.000.000 di dollari (19).

Secondo alcuni esperti la perdita totale annua dovuta ai crimini in questione ammonta a 100.000.000 di dollari, mentre secondo altri essa va da 200.000.000 a 300.000.000 di dollari (20).

In qualche caso la perdita accertata è stata di 5.000.000 di dollari mentre in un caso, quello della Equity Funding Corporation of America, di cui tratteremo più diffusamente in seguito, la perdita totale ha raggiunto l'astronomica cifra di 2.000.000.000 di dollari.

4. — La definizione di *computer-crime* è controversa tra gli Autori che si sono occupati dell'argomento.

Secondo TIEDEMANN, il quale però preferisce parlare di delitto nel campo dell'informatica, tale delitto riguarda in generale qualsiasi azione illegale nella quale il computer è lo strumento o l'oggetto del delitto: in altri termini deve trattarsi di un delitto il cui mezzo o il cui scopo siano quelli di influire sul funzionamento di un computer. Tuttavia l'Autore in questione ritiene che la definizione di « delitto d'informatica » richieda una definizione più precisa ed afferma che esso si con-

---

(17) PARKER *op. cit.* alla nota 3), p. 38. Vedi sullo argomento, COMPTROLLER GENERAL OF THE UNITED STATES, *Computer-related Crimes in Federal Programs. Report to the Congress*, Washington '76.

(18) *The Cost of Crimes Against Business*, cit. alla nota 16).

(19) PARKER, NYCUM, OÜRA, *Computer Abuse*, S. R. I., novembre 1973.

(20) PARKER, *op. cit.* alla nota 3), pag. 29.

creta in « qualsiasi delitto contro i beni collegato al trattamento automatico dei dati » (21).

PARKER, a sua volta, preferisce parlare di *computer abuse* piuttosto che di *computer-crime*, intendendo con esso qualsiasi atto criminoso associato con la tecnologia del computer nel quale una vittima ha subito una perdita ed un autore ha intenzionalmente ricavato un guadagno (22).

Secondo altri Autori, per distinguere un *computer-crime* da un crimine tradizionale occorre scendere sul terreno pratico: esaminare, cioè, se il crimine commesso avrebbe potuto, oppure no, essere portato a termine con la stessa intensità e la stessa estensione anche qualora il computer non vi fosse stato coinvolto (23).

Premesso ora che lo sviluppo della tecnologia e l'emergere in questo campo di sempre nuove forme di specifica criminalità rendono molto difficile la formulazione di definizioni esatte, ritengo che si possa fondatamente parlare di una categoria generale di *computer-crimes*, nella quale rientra qualsiasi comportamento criminoso in cui il computer è stato coinvolto o come mezzo materiale o come oggetto dell'azione criminosa ovvero come mezzo simbolico.

In quest'ultimo caso l'autore si avvale per la commissione del crimine sostanzialmente della convinzione erronea della vittima circa la infallibilità dei dati del computer; ciò per procurarsi vantaggi psicologici o per ingannarla.

Nell'ambito della categoria generale possono poi effettuarsi delle suddivisioni, tenendo presente non più il ruolo giocato dal computer nella produzione dell'evento, bensì lo scopo dell'azione criminosa.

Possono in tal modo distinguersi:

1. crimini correlati all'uso del computer ed aventi per scopo la realizzazione di un profitto per l'autore e/o la produzione di un danno, inteso il termine in senso ampio, per la vittima;

---

(21) TIEDEMANN, *Phénoménologie des infractions économiques*, in *Aspects criminologiques de la délinquance d'affaires*, Strasbourg, 1978, p. 231, ss.

(22) PARKER, *op. cit.* alla nota 3), p. 12.

(23) LEIBHOLZ-WILSON, *Users' Guide to Computer Crime*, Radnor, Pennsylvania, 1974, p. 14.

Sull'argomento vedi anche, LAMPE, *Die strafrechtliche Behandlung, der sog. Computer Criminalität*; Goldammer's Arch. Strafr., 1975, 1.

2. crimini diretti contro il computer come entità fisica, aventi cioè per scopo la distruzione o il danneggiamento in tutto o in parte del sistema e/o dei suoi prodotti (dati e programmi);

3. crimini correlati all'uso del computer e diretti a procurare (o concretantisi nella minaccia di procurare) danni fisici ad individui o gruppi.

Nell'ambito della sottocategoria di cui al n. 1 rientrano:

a) l'appropriazione dei dati, dei programmi e delle informazioni del computer; b) il furto di servizi; c) l'appropriazione di beni materiali; d) i c.d. crimini finanziari.

Nella sottocategoria di cui al n. 2 rientrano, invece:

a) il sabotaggio industriale; b) il sabotaggio politico; c) il vandalismo.

Infine nella sottocategoria di cui al n. 3 rientrano:

a) l'assassinio o la minaccia di esso; b) la strage o la sua minaccia (23 bis).

Occorre ora procedere all'esame delle singole fattispecie.

Per quanto riguarda i casi di cui sub a) è da dire che i dati, le informazioni ed i programmi, oltre che sottratti, possono essere anche manipolati ai fini della commissione del delitto. Il furto consiste nella sottrazione o nella riproduzione di un programma importante dal punto di vista economico o aziendale o, comunque, di informazioni e dati importanti (ad es. inventari di merci, ecc.).

In Olanda, ad esempio, un programmatore della Imperial Chemical Industries (ICI), una delle più grandi industrie europee, approfittando di un *week-end*, ha sottratto alcune centinaia di bobine contenenti programmi del computer della società, cagionando un danno di oltre 100.000 dollari.

In Svezia due impiegati hanno venduto dati bancari riservati della loro ditta ai concorrenti della stessa, così come un impiegato di New York City ha venduto una lista di clienti importanti della sua ditta ad una ditta concorrente (24).

---

(23 bis) Sulle varie forme di «*computer crime*» vedi anche BEQUAI, *Organized Crime in the Computer Arena*, *Cit.* alla nota 3), p. 24, ss.: idem, *op. cit.* alle note 6) e 9), p. 106; PARKER, *op. cit.* alla nota 3), p. 17; TIEDEMANN, *La criminalité socio-économique*, ecc., in *Rev. sciences crim.* 1974, p. 749; idem, *op. cit.* alla nota 21); SIEBER, *Computerkriminalität und Strafrecht*, Köln, 1974.

(24) BEQUAI, *op. cit.* per prima alla nota 23 bis).

Tre operatori del computer dell'Enciclopedia Britannica si sono appropriati di una lista contenente circa 3.000.000 di nominativi di clienti importanti e l'hanno venduta alle società concorrenti, realizzando una grossa somma (25). Esiste già, in effetti, un vasto mercato nero — nazionale ed internazionale — di dati importanti derivati dal computer e delinquenti specializzati giocano un ruolo importantissimo nello sviluppo di siffatto mercato. Gli acquirenti di programmi possono appartenere sia a delle società rivali che a Paesi stranieri (26).

In ordine ai programmi occorre tenere presente che essi richiedono spesso anni per la loro redazione e messa a punto da parte degli analisti e dei programmatori e frequentemente sono molto costosi. Qualche programma può costare anche milioni di dollari (27).

Una forma particolare di furto è il c.d. spionaggio economico. Lo spionaggio economico nel settore in esame concerne l'acquisizione illegale preordinata di informazioni concernenti le ricerche, i progetti di costruzione, le liste dei clienti, l'organizzazione di vendita, ecc. di una società che opera con lo EDP. Esso è facilitato dal fatto che i dati relativi sono contenuti in uno spazio ridottissimo e possono essere immediatamente trasferiti su altri supporti, specie su bande magnetiche.

Il tipo di crimine in questione è praticato largamente anche da agenti di Paesi del blocco orientale.

A Berlino Est, ad esempio, sin dal 1966 era stato messo a punto un piano a lungo termine che comprendeva un addestramento di base in tema di informatica di agenti del Servizio Segreto ed il perfezionamento degli stessi nella Germania Federale. Una serie di spettacolari processi per spionaggio economico in effetti è stata celebrata in quest'ultimo Paese. In particolare, alla fine del 1974, un procedimento penale è stato aperto contro 12 persone che avevano fornito copie di istruzioni di funzionamento, di sistemi e programmi, nonché bande e dischi magnetici ad una organizzazione di Servizi Segreti dell'Est, operante sotto apposita copertura (28).

---

(25) BEQUAI, *op. cit.* alla nota 6).

(26) BEQUAI, *op. cit.* alla nota 24).

(27) PARKER, *op. cit.* alla nota 3), p. 154. Vedi anche BORRUSO *op. cit.* alla nota 2, vol. I, pag. 32.

(28) TIEDEMANN, *op. cit.* alla nota 21, p. 235.

L'ipotesi di cui alla lettera *b*) riguarda l'uso del tempo di lavoro del computer a spese della società. Al riguardo è da tenere presente che i computers sono stati spesso usati da impiegati per condurre i loro personali affari e l'illecito è in continuo aumento. A Filadelfia, per esempio, negli anni precedenti il 1977, dei programmatori della « Sperry-Univac » si sono serviti del computer della società per preparare sofisticati arrangiamenti musicali (29).

L'illecito ha, peraltro, invaso anche il settore pubblico. Si sono scoperti casi nei quali i politici locali usavano il computer municipale per spedire la propria posta a fini elettorali (30).

In genere, però, le Università ed i *Computer Service Centres* sono le vittime privilegiate degli illeciti in questione. Va posto in rilievo, al riguardo, che il furto di servizi può provocare danni considerevoli alla organizzazione interessata. L'utilizzazione di un sistema complesso di computers può costare, infatti, oltre 1.000.000 di lire all'ora e, se si tratta di un sistema dato in locazione — il costo del quale, cioè, è determinato dalla effettiva utilizzazione delle apparecchiature — il pregiudizio arrecato alla società locataria può essere molto pesante. Un illecito di questo tipo commesso in un grande Ufficio di ingegneria è costato alla società circa 2.800.000 dollari (31).

In merito al furto di beni (lett. *c*) è da tener presente che il criminale semplicemente manipolando il computer può realizzare considerevoli somme. Qualsiasi computer di una società può essere programmato per acquistare o spedire merci o altri beni. Nella Corea del Sud il computer dell'Armata Americana è stato usato per derubare l'esercito di costose attrezzature del valore di oltre 10.000.000 di dollari, mediante la cooperazione di elementi della malavita coreana e di quella americana (32).

Si aggiunga che le stesse componenti del EDP possono costituire un bene patrimoniale in sé e quindi essere sottratte.

A Miami, Florida, il Federal Grand Jury ha condannato due spie le quali avevano sottratto parti importanti di computers, esportandole poi nei loro Paesi.

Come abbiamo già detto, i computers rendono possibile ai criminali l'appropriazione di grandi quantità di merci o di altre

---

(29) BEQUAI, *op. cit.* alla nota 24).

(30) BEQUAI, *op. cit.* alla nota 5), p. 106.

(31) TIEDEMANN, *op. cit.* alla nota 21), p. 236.

(32) BEQUAI, *op. cit.* alla nota 23).

cose mediante semplici manipolazioni del sistema. Allorché il criminale, infatti, riesce ad avere accesso al computer di una società che effettua vendite commerciali, egli può fare grossi ordinativi di merce e dare istruzioni al computer medesimo per la consegna della stessa in determinati posti, senza destare eccessivi sospetti in quanto la prassi commerciale americana considera normale una perdita annua di inventario tra il 3 per cento e il 5 per cento.

Il caso riferito qui di seguito dimostra come le possibilità di cui sopra siano concrete, così come dimostra la scarsa efficienza o la trascuratezza in ordine all'apprestamento di elementari cautele da parte delle società proprietarie dei computers.

Agli inizi degli anni '70, rovistando nei contenitori di rifiuti della *Pacific Telephone Company* di Los Angeles, California, uno studente esperto di sistemi elettronici, Jerry Schneider, rinvenne una serie di documenti riguardanti l'organizzazione, il sistema di vendita ed il funzionamento del computer della Compagnia (un IBM-360) l'oggetto della quale era la vendita di materiale telefonico.

Le filiali della Compagnia ordinavano il materiale necessario presso la sede centrale utilizzando un sistema di chiamata per pulsanti denominato *Touch-Tone-Dial* collegato per telefono al computer centrale della PTC.

Il criminale riuscì ad apprendere il codice del computer telefonando sotto falso nome ad una delle filiali. Utilizzando un telefono *touch-tone*, Schneider, per sette mesi nel 1971, ordinò la consegna di varie partite di materiale telefonico per un valore complessivo di circa 1.000.000 di dollari.

Soltanto alla fine del 1971, a seguito della « soffiata » di un complice, e quindi per puro caso, la frode venne scoperta (33): il criminale venne condannato alla lieve pena di due mesi di reclusione più tre anni di « probation ».

Vi sono poi i crimini finanziari compiuti attraverso il computer. Gli illeciti riguardano la manipolazione dei dati relativi a libri paga, partite attive e passive, ecc. Il crimine può prendere varie forme. Di solito il criminale sottrae somme o documenti negoziabili. Tuttavia, attraverso la semplice manipolazione del computer di una società si possono anche creare capitali e gua-

---

(33) TIEDEMANN, *op. cit.* alla nota 21); PARKER, *op. cit.* alla nota 3), p. 59, ss.

dagni fittizi. I membri del crimine organizzato potrebbero facilmente ingannare i creditori di società da loro controllate facendo apparire che la società è, contrariamente al vero, finanziariamente solida, e in tale modo preparare il terreno per una successiva massiccia frode fallimentare (34).

Il sabotaggio industriale consiste in un attentato all'EDP di una società, normalmente ordinato da parte di una società concorrente, allo scopo di danneggiare la stabilità economica della vittima. L'obiettivo, cioè, è quello di distruggere o bloccare le capacità operative della vittima, neutralizzando le sue capacità competitive nel campo delle forniture private e delle forniture pubbliche. Il sabotaggio industriale può essere anche praticato su disposizione di aspiranti acquirenti di una società i quali, provocando una crisi dell'organizzazione della medesima, possono poi acquistare la società stessa a basso prezzo (35). Le perdite per sabotaggi del genere sono nell'ordine di milioni di dollari annualmente.

L'attacco al computer per motivi politici (sabotaggio politico) è anche molto frequente e, per gli obiettivi presi di mira (Centri pubblici di dati ed informazioni, Centri di difesa militare, ecc.), appare estremamente pericoloso e dannoso. Negli Stati Uniti sono stati attaccati i computers di una delle più grandi basi aeree della Nazione così come un complesso sistema di computers, dato in locazione al Pentagono. Anche il computer di una Università che lavorava per compiti attinenti alla difesa nazionale è stato attaccato con esplosivi ed ha sofferto più di 2.000.000 di dollari di danni.

La *Daw Chemical Company*, un tempo obiettivo di azione di un gruppo di opposizione alla guerra nel Vietnam, ha subito l'invasione del suo *computer center*. I danni hanno raggiunto il milione di dollari.

Nell'agosto del 1970 dei gruppi anti-militaristi e terroristi hanno distrutto, a mezzo esplosivo, le informazioni raccolte in un periodo di circa 20 anni dal Centro di ricerche matematiche dell'Esercito presso l'Università del Wisconsin (36).

Nel 1968 un ignoto criminale ha colpito con un'arma da fuoco l'IBM 1.401 dello *State Unemployment Office* in Olimpia,

---

(34) BEQUAI, *op. cit.* alla nota 23).

(35) BEQUAI, *op. cit.* alla nota 21), p. 23.

(36) PARKER, NYCUM, OÜRA, *Computer Abuse*, Stanford Research Institute, 1973, p. 3; FARR, *The Electronic Criminal*, N.Y. 1975, p. 44.

Washington. Nel 1972 un computer *tax processing* della città di Johannesburg, Sud Africa, è stato ugualmente colpito con armi da fuoco.

In Australia, a Melbourn, dimostranti antimilitaristi hanno attaccato con armi nel 1973 il computer di una Compagnia manifatturiera, distruggendolo totalmente. In uno Stato dell'Est, nel 1974, un operatore di computer, infuriato nei confronti di quest'ultimo, lo ha attaccato durante la notte con un'arma da fuoco, danneggiandolo seriamente (37).

Nel Regno Unito dei terroristi hanno ripetutamente attaccato un computer della Polizia ed in Africa dei sabotatori, nell'attacco ad altro computer, hanno ucciso molti degli addetti al sistema (38).

Anche in Italia i gruppi terroristi hanno preso di mira i computers. Agli inizi del dicembre del 1978 le Brigate Rosse hanno attaccato ed incendiato il Centro Elaborazione Dati della Direzione Generale della Motorizzazione Civile e dei Trasporti, causando notevolissimi danni per la distruzione di importanti dati. Il giorno successivo, poi, è stato attaccato, fortunatamente senza conseguenze, il computer della Banca del Monte di Bologna e Ravenna.

Passando ora a parlare del vandalismo, è da dire che esso consiste in danneggiamento del computer, o di suoi prodotti, compiuti da impiegati scontenti o in sciopero. Gli impiegati sono ben conosciuti per una certa propensione a dar fuoco ai *computer centers*. Recentemente, in uno Stato dell'Unione, un impiegato ha sparato contro il computer della ditta con un'arma automatica. In un altro caso, un operatore dell'EDP ha distrutto i dati contabili relativi a crediti della ditta verso clienti, cagionando in tal modo qualche milione di dollari di danni per fatture non pagate (39). L'asportazione di tutte le etichette relative a 1.500 bobine di un computer da parte di un impiegato ha comportato ad una società grandi spese e l'impiego di moltissimo tempo per la reidentificazione dei dati (40).

Infine un impiegato di una Compagnia di Assicurazioni, per vendicarsi del suo licenziamento, ha cancellato tutte le bande

---

(37) PARKER, *op. cit.* alla nota 3), p. 285).

(38) BEQUAI, *op. cit.* alla nota 23).

(39) BEQUAI, *op. cit.* alla nota 23).

(40) BEQUAI, *op. cit.* alla nota 5), p. 106).

magnetiche del computer della Compagnia, cagionando circa 10.000.000 di dollari di danni (41).

Infine, il computer può essere usato dai criminali anche per arrecare danno a singoli individui in quanto persone fisiche o anche a collettività.

Come è noto, i computers sono adoperati in numero crescente in molti ospedali in sistemi di *Life-Support*, così come sono usati in numerosi laboratori e in grandi sale operatorie. Attraverso le manipolazioni dei relativi computers i criminali potrebbero cagionare la morte di una persona. Basterebbe all'uopo sabotare il computer di un complesso di rianimazione *Life-Support*.

Va poi tenuto presente che i missili nucleari ed altri mezzi bellici di distruzione sono controllati e diretti dai computers. Elementi criminali potrebbero agevolmente cambiare quei computers in mezzi di devastazione o di terribile ricatto nei confronti di città e Nazioni. Per dirla con BEQUAI, il computer potrebbe diventare il nuovo « Hit-man » del XX Secolo (42).

5. — In genere l'EDP è un sistema con quattro aree fondamentali di operazioni la cui conoscenza, sia pure sommaria, appare indispensabile per comprendere le modalità di commissione dei *computer-crimes*. Esse riguardano le fasi dell'« input », della programmazione, dell'« output » e della comunicazione dei dati.

La fase dell'« input » è la prima fase delle operazioni di un computer: in essa le informazioni sono tradotte in un linguaggio intellegibile per il computer medesimo. Le persone che vi hanno accesso possono facilmente manipolare il sistema inserendo semplicemente dati falsi. Esse possono anche alterare le informazioni ed eliminare documenti-chiave di entrata. La manipolazione dei dati « input » costituisce una delle forme più comuni di *computer-crime*.

I crimini finanziari, in particolare, normalmente hanno il loro inizio in questa fase (43).

Appare opportuno, per una più esatta comprensione del fenomeno, riportare qualche caso. Un impiegato di una grande

---

(41) MCKNIGHT, *Computer Crime*, N.Y. 1973, p. 121.

(42) BEQUAI, *op. cit.* alla nota 23).

(43) BEQUAI, *op. cit.* alla nota 5), p. 108.

fabbrica statunitense fornì al computer della sua Compagnia dati falsi, creando dei fornitori fittizi. In seguito il computer ordinò il pagamento dei loro conti. In meno di due anni la Compagnia perse in questo modo più di 1.000.000 di dollari (44). Il Vice Presidente di una grande ditta manifatturiera americana inserì nel computer dati falsi creando fornitori e trasportatori fittizi ai quali vennero versati in complesso circa 1.000.000 di dollari. Con la complicità dei sopracitati individui, la somma venne incassata e ripartita tra questi ultimi e il dirigente (45).

Recentemente il *District Attorney* della Contea di Nassau (N.Y.) ha annunciato l'arresto dell'ex supervisore contabile della *Gouvernement Employers Insurance Company*. Egli aveva immesso falsi *vouchers* (ricevute di servizi) nel computer della Compagnia ed in conseguenza erano stati emessi una serie di chèques intestati ad una Compagnia fittizia che era sotto il controllo del criminale. L'illecito, come in quasi tutti i casi, venne scoperto fortuitamente (46).

In un'altro caso il cassiere di una grande banca di New York, con l'aiuto di un complice, istruì il computer della banca ad emettere assegni per il pagamento di dividendi a favore di ex azionisti che avevano venduto il loro pacchetto di azioni di una società, ma per i quali la banca era autorizzata ad agire come agente di trasferimento. Gli assegni furono poi incassati dai criminali i quali avevano anche istruito il computer a cancellare i *records* degli assegni dopo la loro emanazione (manipolazione combinata « input » ed « output »). Essi furono, come sempre, scoperti per caso a seguito di una « soffiata » (47).

Alla fine degli anni '60, la *Human Resources Administration* di New York lamentò la perdita di circa 2.000.000 di dollari avvenuta durante i primi mesi del 1968 in seguito al fraudolento pagamento di chèques all'*Youth Corp*, con emissione di circa 100 assegni erronei alla settimana (48).

Un altro caso è quello di due donne dichiarate colpevoli per un furto di oltre 400.000 dollari ai danni di un fondo sindacale. Una delle due donne era impiegata presso un Ente che gestiva i fondi delle pensioni di un sindacato e trasmetteva il denaro

---

(44) BEQUAI, *op. cit.* alla nota 5), pag. 108.

(45) BEQUAI, *op. cit.* alla nota 6).

(46) BEQUAI, *op. cit.* alla nota 6).

(47) BEQUAI, *op. cit.* alla nota 6).

(48) LEIBHOLZ-WILSON, *op. cit.* alla nota 23).

alla sua complice compilando semplicemente delle false richieste di benefici, inserite poi nel computer dell'Ente (48 bis).

Anche il settore dell'istruzione è coinvolto nei *computer-crimes*. Nell'agosto 1977 la polizia scoprì in una grande Università americana un piano che prevedeva pagamenti da parte di studenti che desideravano vedere aumentati i loro voti.

L'inchiesta fu promossa a seguito di una serie di lettere indirizzate al personale universitario, specificanti il piano ed i nomi delle persone implicate. Gli investigatori scoprirono che un funzionario dell'Università aveva incassato migliaia di dollari per cambiare le schede dei voti che dovevano essere immesse nel computer universitario (49). Il caso di Jerry Schneider, citato al paragrafo 4), è un altro esempio di manipolazione di dati « input » dimostrante che tali manipolazioni possono essere commesse anche da persone estranee all'organizzazione interessata.

Altri casi di *computer-crimes* hanno interessato la Repubblica Federale di Germania e la Svizzera.

Due impiegati di una società di Amburgo sono riusciti a trasferire più di 300.000 DM sui loro conti personali introducendo delle false fatture nel computer della società medesima. Nel sud della Repubblica Federale di Germania un impiegato dell'Amministrazione, incaricato della ripartizione degli assegni familiari, è stato condannato per truffa in tema d'informatica.

La scheda perforata relativa a tali assegni, che doveva essere trasmessa al computer per autorizzare il pagamento, avrebbe dovuto recare la firma di un altro impiegato, firma che il criminale falsificò riuscendo a trasferire notevoli somme su vari conti a lui intestati. Per nascondere l'illecita operazione, lo stesso impiegato aveva fatto in modo di omettere all'uscita di controllo del computer la prima cifra delle somme trasferite (manipolazione « input » ed « output » combinata). In un periodo di 10 mesi egli riuscì ad effettuare 29 di tali operazioni, appropriandosi complessivamente di più di 250.000 DM (50).

In un'impresa più piccola un operatore ha fatto calcolare al computer della ditta, per moltissimo tempo, il salario di im-

---

(48 bis) BEQUAI, *op. cit.* alla nota 5), p. 105.

(49) BEQUAI, *op. cit.* alla nota 5), p. 108.

(50) TIEDEMANN, *op. cit.* alla nota 21), p. 234.

piegati inesistenti ed ha fatto versare il loro stipendio sul conto di sua moglie (51).

In altri due casi, avvenuti sempre in Germania, degli impiegati hanno raddoppiato i loro stipendi manipolando le cifre nella memoria del computer. Manipolazioni del genere sono state all'origine dell'insolvenza della banca tedesca *Herstatt* con un danno di oltre 200.000.000 DM, e dello spettacolare fallimento dell'*Equity Funding Corporation of America* di cui si dirà più diffusamente in seguito (51 bis).

Anche la Svizzera ha conosciuto dei casi di manipolazione dei dati « input ». In uno di essi il criminale, che era l'operatore capo del dipartimento di informatica dell'Amministrazione fiscale cantonale, effettuò due diversi tipi di manipolazioni tra il 1965 ed il 1969. Egli cominciò con il distruggere le schede perforate di addebito intestate al suo nominativo ed a quello di un amico. Il computer non imprimeva la lettera di richiamo malgrado l'assenza di pagamenti e delle carte di verifica.

In seguito egli preparò per altre sei persone dei dati confermant i il pagamento di somme mai versate. Anche in questo caso il computer ometteva di imprimere le lettere di richiamo (52).

La successiva fase è quella della programmazione. Nel corso di essa vengono fornite al computer delle sequenze logiche di operazioni « step-by-step » per la soluzione dei problemi. Anche qui la casistica degli illeciti è abbondante. Ad esempio, il contabile di una grande ditta alterò il programma del computer in modo tale da aggiungere alcuni spiccioli al costo di molti articoli acquistati. In un arco di 5 anni egli in tal modo « aspirò » 1.000.000 di dollari. Per convertire le entrate sui libri contabili in personale profitto egli creò dei fornitori fittizi e fece emettere a loro favore degli chèques da lui stesso preordinati. Mediante un certo numero di prestanome egli incassò poi i fondi relativi (53).

Il programmatore di un'impresa *software houses* aggiunse al programma del computer di una banca un sotto-programma

---

(51) TIEDEMANN, « *La Criminalité socio-economique: aspects internationaux et de droit comparé* », in *Rev. science crim.*, 1974, p. 749.

(51 bis) SIEBER, in « *Aspects criminologiques de la délinquance d'affaires* », *op. cit.* alla nota 21), p. 19.

(52) ROHNER, *Computerkriminalität*, Zurich 1976, p. 110, citato da TIEDEMANN, *op. cit.* alla nota 50).

(53) BEQUAI, *op. cit.* alla nota 6).

supplementare il quale operava in modo che i suoi prelevamenti allo scoperto non venissero registrati dalla banca. Il crimine fu scoperto per caso in occasione di una « panne » del sistema che obbligò la banca ad effettuare i conti manualmente (54).

Nel 1971 la *New York Penn Central Railroad* scoprì che più di 200 carri ferroviari di sua proprietà, del valore di 60.000 dollari ciascuno, erano stati dirottati dai suoi depositi di Filadelfia ad un nascosto deposito ferroviario nell'area di Chicago nel quale erano poi stati riverniciati con diverso colore. Il Federal Grand Jury accertò che questo sistema era comune e che più di altri 200 carri erano spariti dai depositi della Compagnia. In realtà il computer della Compagnia stessa era stato manipolato ed istruito a dirottare i carri in altre località (55).

Una grande banca di New York è stata derubata ad opera di un programmatore mediante un metodo detto *breakage*. Il termine indica la frazione di un penny o di un dollaro che si è soliti non computare nel calcolo degli interessi. Il criminale fece affluire, tramite il programma del computer, l'ammontare di tali frazioni sul proprio conto realizzando un ingente profitto (56).

I programmi comunque, oltre ad essere manipolati, possono essere anche, come abbiamo già detto, sottratti e rivenduti e perfino diventare oggetto di estorsione.

In tema di sottrazione di programmi, il maggior *computer-crime*, a parte quello della *Equity Funding*, risale al 1964 allorché un programmatore del Texas sottrasse alla sua ditta programmi del valore di alcuni milioni di dollari, rivendendoli ad un cliente della sua stessa ditta (57).

Come si è già detto, i programmi possono anche essere sottratti a scopo di estorsione. Alcuni anni fa dei malviventi rapinarono la succursale di Los Angeles della *Bank of America* portando via, tra l'altro, anche varie bande magnetiche del computer. Quando ne scoprirono il valore, richiesero il pagamento di un riscatto (58). Nel 1977 un manager venticinquenne della filiale olandese della *Imperial Chemical Industries* (ICI) addetto al *Computer Centre*, sottrasse circa 1.000 libbre di dischi

---

(54) PARKER, NYCUM, OÜRA, *op. cit.* alla nota 19), p. 37; FARR, *op. cit.* alla nota 35), p. 44.

(55) BEQUAI, *op. cit.* alla nota 9), p. 1.

(56) LEIBHOLZ-WILSON, *op. cit.* alla nota 48), p. 12.

(57) LEIBHOLZ-WILSON, *op. cit.* alla nota 48), p. 29.

(58) BEQUAI, *op. cit.* alla nota 5), p. 103.

magnetici del computer, contenenti i futuri programmi della compagnia, e richiese poi un riscatto di 400.000 dollari (59).

La terza fase è quella dell'« output », durante la quale le informazioni provenienti dal CPU, e cioè dalla memoria del computer, sono tradotti in linguaggio intelligibile all'uomo. PHILIP MANUEL, un senatore inquirente americano che ha studiato per anni il problema della sicurezza dei computers, ha accertato che più del 90% dei computers del settore pubblico e di quello privato sono vulnerabili in questa fase ad eventuali illeciti (60). I crimini più frequenti nella fase in questione riguardano il furto delle informazioni privilegiate: più propriamente di *printouts*, di liste di spedizione, di elenchi di indirizzi postali, di inventari, di liste di clienti e di dati confidenziali di « marketing », di segreti industriali in genere, e di segreti militari. I dati sottratti, come già detto, vengono poi venduti al sempre più fiorente mercato nero ed acquistati da ditte concorrenti o anche da potenze straniere. I casi seguenti riguardano illeciti commessi in questa fase. Un operatore del computer di una ditta di media grandezza preparò un duplicato di un tesserino a tempo (*time-card*) relativo ad un impiegato del settore spedizione. Egli elaborò poi i dati attraverso la regolare partita di stipendio, istruendo però il computer ad omettere alcuni dettagli del secondo pagamento. In seguito l'operatore falsificò la firma dell'impiegato ed incassò l'assegno con una seconda girata, ripetendo l'operazione molte volte e scegliendo nominativi di impiegati di differenti settori, in tal modo minimizzando la possibilità che i singoli impiegati potessero notare delle irregolarità nell'estratto conto dei loro redditi annuali (61).

Nel 1971, nella Germania Occidentale si scoprì che un agente della Germania dell'Est era riuscito a copiare dati finanziari confidenziali e dati di produzione relativi a 3.000 società della Repubblica Federale riprodotti su bande magnetiche, fornendo poi le notizie al Governo del suo Paese (62). Gli esperti ritengono che il crimine organizzato ha già preso possesso di questa area.

L'ultima fase delle operazioni di un computer è quella della comunicazione dei dati, la quale implica l'uso di circuiti tele-

---

(59) BEQUAI, *op. cit.* alla nota 9), p. 55.

(60) BEQUAI, *op. cit.* alla nota 5), p. 108.

(61) BEQUAI, *op. cit.* alla nota 6).

(62) LEIBHOLZ-WILSON, *op. cit.* alla nota 48), p. 37.

fonici per trasmettere le informazioni dal computer ai terminali e viceversa, oltre che da un computer all'altro.

L'intercettazione dei dati può assumere varie forme. Vi è anzitutto la possibilità, qualora il computer non identifichi l'entrata dal terminale, di collegare un terminale non autorizzato attraverso il quale il criminale può non soltanto prendere conoscenza dei dati ma anche eventualmente manipolarli. Il sistema è noto sotto il nome di *browsing* (63).

Un serio problema che l'F.B.I. ha dovuto spesso affrontare è quello relativo al cosiddetto *Phone freak* attuato attraverso lo uso di un terminale remoto. Esso si concreta in un'entrata abusiva nel sistema a scopo di sfida. Ad esempio, nel New Jersey si scoprì che, attraverso uno dei terminali donati ad una scuola da parte di una ditta produttrice di computers, gli studenti avevano eluso il codice di sicurezza del computer della ditta donatrice ed avevano istruito il computer medesimo a stampare la frase: « va a... Il fantasma » (64). La penetrazione elettronica nel sistema può essere attuata in diversi modi. Uno dei metodi più comuni è quello detto *Wiretap* e consiste nel collegare una « presa » direttamente alla linea telefonica usata per le comunicazioni: i messaggi intercettati sono poi registrati. Più sofisticati sono gli altri sistemi. Vi è anzitutto il *Piggyback entry* adoperato per intercettare i messaggi tra il computer ed un terminale e per alterarli mediante aggiunte o cancellazioni. Modificando i dati il delinquente riesce, di fatto, ad influenzare il processo decisionale dell'utente. Altro sistema sofisticato è quello detto *Electromagnetic pickup* mediante il quale si intercettano le radiazioni emesse da un computer, da un telefono o da una telescrivente, senza collegamenti diretti al sistema. Infine un modo più comodo di penetrazione è quello denominato *Between-the-lines-entry*. Esso viene attuato sfruttando la linea di un utente autorizzato. Il criminale entra nel sistema ogni volta che l'utente legale è inattivo, mantenendo però in funzione il canale di comunicazione (65).

6. — Il caso spettacolare di frode commesso da alcuni dirigenti ed operatori della Compagnia di assicurazione *Equity Funding Corporation of America* merita una trattazione più dif-

(63) BEQUAI, *op. cit.* alla nota 6).

(64) BEQUAI, *op. cit.* alla nota 9), p. 81.

(65) BEQUAI, *op. cit.* alla nota 9), p. 12.

fusa. I crimini commessi dai 21 imputati furono di varia natura ma tra essi spiccava il più grave «computer crime» mai commesso negli Stati Uniti. Il fatto è stato definito da FARR «*the most monumental money swindle of modern times*» ed è stato oggetto di studi e rapporti tra cui quello, voluminosissimo, del curatore del successivo fallimento della Compagnia (66). Si è trattato di un classico crimine finanziario commesso «*by computer*».

I criminali iniziarono, a partire dalla fine degli anni '60, a creare polizze di assicurazioni false fino a giungere ad un totale di 56.000 polizze false su un totale di 91.000 gestite dalla Compagnia. Tali polizze (false) venivano poi rivendute ad altre compagnie di assicurazione. I contratti erano fatti in modo che i premi non avrebbero dovuto essere pagati dai fittizi assicurati bensì da parte di un Fondo di investimenti di una filiale dell'EFCA. Gli acquirenti si accontentarono dei documenti forniti dal computer come prova dell'esistenza delle polizze acquistate, il che permise ai criminali di introdurre dati falsi nel computer utilizzando a questo fine dei dati provenienti da polizze estinte. Con l'aiuto di un apposito programma, i numeri delle vecchie polizze furono modificati ed i premi e le somme da pagare moltiplicate per 1,8 (67).

Le false polizze avevano un numero di codice convenzionale e cioè «*Department 99*» che consentiva al computer di escluderle allorché le polizze dovevano essere inviate agli assicurati. Al momento dei controlli da parte dei funzionari governativi, e cioè allorché questi chiedevano la documentazione in ordine alle polizze, il personale della Compagnia guadagnava tempo, dichiarando che i «dossier» non erano disponibili al momento. Subito dopo venivano creati «dossier» contenenti vari atti, e cioè certificati medici, contratti, ecc. Il giorno successivo la richiesta degli investigatori veniva così esaudita.

L'enorme e complessa frode venne alla luce allorché nel 1973 uno dei complici venne licenziato e spifferò tutto (68). La perdita raggiunse l'astronomica cifra di 2.000.000.000 di dollari

---

(66) LOEFFLER, «*Report of the trustee of Equity Funding Corporation*», 1974. Vedi anche in particolare SOBLE-DALLAS, *The Impossible dream. The Equity Funding Story: The fraud of the Century*, C. P. Putnam, 1975; GRIMES, *Equity-Funding: Fraud by Computer*, American Federationist 80, dicembre 1973, p. 7-9.

(67) TIEDEMANN, *op. cit.* alla nota 21), p. 239.

(68) BEQUAI, *op. cit.* alla nota 5), p. 107.

ma, nonostante l'enorme scandalo, i colpevoli beneficiarono di condanne miti. Il processo penale fu seguito da una serie di processi civili intentati da molti « *Equity Investor* » e dalla stessa società collegata, la *Equity Funding Life Insurance Company* contro l'IBM, produttrice del computer in dotazione alla EFCA. Gli attori richiesero un risarcimento di danni per complessivi 4.000.000.000 di dollari sostenendo la colpa dell'IBM la quale aveva omesso sia di informare i clienti della vulnerabilità del sistema sia di munire il sistema stesso delle opportune misure di sicurezza.

7. — Dati interessanti sui tratti psicologici degli « *electronic criminals* » si ricavano da elementi emersi nei processi celebrati negli Stati Uniti e nella Repubblica Federale di Germania. Dal punto di vista anamnastico, si tratta di persone che appartengono alla classe di età che va dai 24 ai 33 anni (69), e cioè di giovani, che appaiono istruiti, educati, di razza bianca, curati nella persona in genere, appartenenti nella quasi totalità al sesso maschile.

Per quanto riguarda la struttura della personalità dei « *computer criminals* », PARKER, dopo aver attentamente studiato ed intervistato un certo numero di essi, è giunto alla conclusione che il *computer criminal*, almeno nell'ambiente americano, è un individuo sveglio, impaziente, molto motivato, audace ed avventuroso, disposto ad accettare la « sfida tecnologica » ((70).

I criminali, almeno nei casi scoperti negli U.S.A. ed in Germania, tendono a cambiare spesso d'impiego nel corso della loro carriera (71). Per quanto riguarda poi il loro atteggiamento nei confronti del crimine, secondo PARKER, essi appaiono affetti dalla c.d. « *sindrome di Robin Hood* ». Il criminale tende a di-

---

(69) Rileva esattamente TIEDEMANN (*op. cit.* alla nota 21, p. 237) che questa classe di età è tipica della fine degli anni sessanta e dell'inizio degli anni settanta giacché in quel momento è iniziato il grande sviluppo dell'informatica.

Per necessità si dovette reclutare il personale dello EDP soprattutto tra i giovani specialisti, e cioè tra individui senza solidi legami con una precedente professione.

(70) PARKER, *op. cit.* alla nota 3), p. 45; vedi anche BEQUAL, *op. cit.* alla nota 9), p. 4. Sui caratteri della vita attiva dei delinquenti « *White Collar* », vedi anche lo studio dei GLUECK, citato in BOUZAT-PINATEL, *Traité du droit pénal et de criminologie*, Paris, 1970, vol. II, p. 395.

(71) TIEDEMANN, *op. cit.* alla nota 21), p. 237.

stinguere tra il far del male ad una persona, ciò che egli ritiene immorale, ed il fare del male ad una organizzazione, ciò che egli crede non sia immorale in certe situazioni (72).

Vi è poi un elemento, per così dire ambientale, che potrebbe — ad avviso di PARKER — convalidare la teoria di SUTHERLAND delle « associazioni differenziali » (73). Secondo questa teoria, l'atto del delinquente tende a deviare soltanto di poco rispetto ai comportamenti comunemente adottati dal suo gruppo.

Orbene da una indagine eseguita negli Stati Uniti mediante la somministrazione di un articolato questionario, nel quale erano elencati i più comuni atti illeciti in tema di uso del computer, ad un gruppo di « managers » e « programmers », è risultato che una parte, spesso notevole, di quest'ultimi non considerava illegali alcuni comportamenti che apparivano, viceversa, oggettivamente illegali, quali — ad esempio — l'accettare ed usare un programma fornito da un amico che lavorava per un'altra società, il cambiare un programma con un altro senza autorizzazione, l'usare per divertimento un terminale diverso da quello ammesso secondo il manuale d'utenza o infine l'accettare la sfida offerta da un servizio « *time-sharing* » per superare i dispositivi di sicurezza di un computer, ecc. Da questo punto di vista il « *computer criminal* » sembra rientrare nella più generale categoria degli « *white collar criminals* » i quali, come è noto, almeno nella stragrande maggioranza dei casi, sono consapevoli del carattere illecito dei loro atti ma appaiono convinti che essi siano delle semplici irregolarità, non dei crimini.

Per quanto riguarda la carriera criminale dei soggetti è da dire che nessuno dei « *computer criminals* » tedeschi aveva precedenti penali (74) mentre pochissimi degli americani avevano subito precedenti condanne (75). In molti casi essi apparivano come « rispettabili cittadini » i quali avevano avuto « sufficienti motivi » per commettere i crimini loro addebitati.

In ordine ai motivi a delinquere, è stata individuata la seguente tipologia, la quale sembra caratterizzare il « *computer criminal* » rispetto al « *white-collar criminal* »: a) desiderio di vendetta da parte di un impiegato licenziato o scontento (van-

---

(72) PARKER, *op. cit.* alla nota 3, p. 46.

(73) SUTHERLAND, *Differential Association*, in *Crime and Delinquency*, London 1970, p. 252.

(74) TIEDEMANN, *op. cit.* alla nota 21), p. 239.

(75) FARR, *op. cit.* alla nota 35), p. 9.

dalismi, sabotaggi, estorsioni); *b*) desiderio di « essere qualcuno »; *c*) difficoltà finanziarie personali; *d*) desiderio di provare a se stesso di essere superiore al « dannato computer » (frustrazioni derivanti dell'interazione « operatore-macchina » (76).

Sembra comunque che gli elementi « rischio » e « sfida » siano molto comuni come spiegazione del comportamento dei *computer-criminals* americani. Una generale caratteristica degli operatori e dei programmatori di computers, infatti, è che essi appaiono affascinati dalla sfida del computer e tanto desiderosi di accettarla da porre spesso in ombra la questione di moralità.

L'idea che un atto in sé illecito sia semplicemente un gioco, una innocua partita giocata con il computer, è spesso accettata nell'ambito degli operatori di un EDP (77). A questa conclusione giunge anche TIEDEMANN il quale però distingue tra i casi verificatisi negli Stati Uniti e quelli accertati in Germania. Nei primi la motivazione prevalente sembra essere stata quella sopra riportata, nei secondi il motivo era unicamente la bramosia del guadagno (78).

Un'altra caratteristica che si riscontra nei « *computer crimes* » e che sembra differenziare questi ultimi dalla criminalità « *white-collar* » in genere è l'alta frequenza di associazione nel reato. Nei casi ordinari di *white-collar crimes*, cioè, la complicità ha una scarsa incidenza. Secondo le indagini di PARKER, su 111 casi di tradizionali frodi o truffe bancarie comportanti perdite sopra i 10.000 dollari, scoperti nel 1971, soltanto 13 comportavano concorso nel reato. Nelle frodi e truffe collegati al computer, invece, almeno la metà dei casi è stata commessa in concorso di due o più persone. In qualche caso i concorrenti erano 6 o 12, in altri 22, in altri ancora oltre 30. Infine in un caso i complici sono stati addirittura 64.

Tuttavia soltanto in 3 casi su 175, l'accordo criminoso riguardava programmatore ed operatore. Ciò è stato spiegato con l'esistenza di un normale diffuso antagonismo tra le due categorie, le quali spesso assumono ruoli antagonistici (79).

(76) FARR, *op. cit.* alla nota 35), p. 9. Secondo LEIBHOLZ-WILSON i « *computer crimes* » sono spesso commessi per uno dei seguenti motivi, o per una combinazione degli stessi; guadagno economico, vantaggi di competizione, desiderio di arrecare danno alla Compagnia (*op. cit.* alla nota 68), p. 17.

(77) PARKER, *op. cit.* alla nota 3), p. 47.

(78) TIEDEMANN, *op. cit.* alla nota 21), p. 239.

(79) PARKER, *op. cit.* alla nota 3), p. 50-51.

8. — La pericolosità sociale dei *computer crimes* è sottolineata da tutti gli Autori che si sono occupati dell'argomento. Tale criminalità invero è caratterizzata dal fatto che: a) il crimine si svolge in un lungo arco di tempo, mentre tale continuità manca in genere o è limitata nei crimini patrimoniali tradizionali; b) la distanza che separa la commissione dell'atto dai suoi effetti rende la scoperta del crimine ancora più difficile; c) il danno arrecato dal crimine è generalmente molto elevato; d) esistono gravi difficoltà nel perseguimento dei crimini stessi.

Va considerato inoltre che il *computer-crime* è relativamente facile da commettere per una serie di ragioni poste in luce da un'indagine condotta dal *Department of Commerce* statunitense (80). Essi sono principalmente: a) l'atteggiamento del « *top management* » di disinteresse, per un difetto di comprensione, del funzionamento dell'EDP; b) la centralizzazione degli elementi del sistema, il che rende le fasi del procedimento facilmente manipolabili; c) la mancanza in genere di documenti cartacei, il che elimina spesso le tracce della commissione del crimine; d) la scarsa attenzione dei fabbricanti di computers e degli utenti in ordine alla predisposizione di misure di sicurezza; e) la trascuratezza degli utenti in ordine alla assunzione, all'addestramento ed al controllo degli operatori in genere dell'EDP, ed in particolare di coloro che hanno accesso diretto al sistema.

In effetti il *computer crime* è quasi impossibile da scoprirsi. Quando ciò è avvenuto, la scoperta è stata dovuta, nella stragrande maggioranza dei casi, ad una « soffiata » o ad una « panne » del sistema il che ha costretto gli operatori ad effettuare le operazioni manualmente. Vi sono poi ragioni di carattere psicologico che inducono gli utenti del sistema ad un atteggiamento di incondizionata fiducia nell'EDP e nei suoi prodotti. Tale atteggiamento è fondato sulla *mistica del computer* e deriva dalla convinzione che il possesso di un costoso apparato elettronico, servito da un ben retribuito gruppo di incomprensibili programmatori, equivalga a possedere la « fonte della conoscenza » (81).

---

(80) *The Cost of Crime Against Business*, citato alla nota 26, p. VI. Vedi anche TRAINI, *Management holds Key to security against computer frauds*, in *Security Gazette*, marzo 1971, p. 121.

(81) LEIBHOLZ-WILSON, *op. cit.* alla nota 48), p. 6.

La *mistica del computer* secondo gli Autori si articola sui seguenti corollari:

1 - Computers are created by geniuses: therefore they are geniuses.

È indubbio che la maggior parte delle manipolazioni accertate del computer sono state rese possibili in quanto, come ha rilevato SIEBER, i proprietari dei computers pensavano che questi ultimi fossero infallibili ed hanno trascurato di premunirsi contro le frodi e gli illeciti in genere, collegati all'uso del computer. La situazione è complicata poi dall'atteggiamento delle vittime. Esse infatti tendono a non denunciare gli illeciti collegati al computer giacché il clamore pubblicitario suscitato ha spesso serie ripercussioni sui loro affari. In qualche caso la vittima si è limitata a trasferire gli autori dei crimini ad un altro settore dell'organizzazione e spesso addirittura ha aumentato i loro stipendi perché non rivelassero gli illeciti commessi!! Ciò in quanto è stato calcolato che la vittima dei *computer crimes*, operante soprattutto nel settore commerciale, perde più a causa della pubblicità negativa che a causa dell'atto criminale in sé (82).

9. — Il *computer crime*, una volta scoperto, appare poi di difficile perseguimento, almeno nel sistema legale nord-americano (82 bis) ed in quello tedesco. Ciò in quanto i dati generati dal computer non possono essere, in via generale, considerati come prove ai fini giudiziari.

Il sistema nord americano in tema di prove relativo alle registrazioni contabili-commerciali è fondato attualmente, a livello federale, sul *Federal Business Record Act* del 1930 il quale ha codificato, almeno per le Corti Federali, la vecchia regola di *common law* denominata *shop-book-rule*.

Circa la metà dei singoli Stati dell'Unione hanno adottato in tema di prove una siffatta disposizione (*Uniforme Business Record*). Il principio fondamentale nord-americano, mantenuto anche nelle recenti « *Federal Rules of Evidence* » è quello della « testimonianza umana ».

Un'eccezione a questa regola è fissata dal sopracitato F.B.R. Act il quale consente l'ammissione in giudizio di una documen-

2 - Computers generate tidy reports; therefore they are correct.

3 - Computers are supposed to save labor costs; therefore they are cheap.

4 - Computer can be programmed to answer any question decisively; therefore they answer correctly.

5 - The ADP manager earns twice as much as the chief accountant; therefore he must be twice as smart.

(82) PARKER, *op. cit.* alla nota 3), p. 16.

(82 bis) Sull'argomento vedi anche HEMPHILL-HEMPHILL, *Prosecuting Computer Criminals*, in *Security World*, 1978, 15 (8).

tazione aziendale allorché concorrano i seguenti requisiti: a) le registrazioni devono costituire un fatto di « routine »; b) esse devono essere effettuate contemporaneamente alla operazione o in un ragionevole lasso di tempo; c) esse devono essere state effettuate da una persona che non possa poi agire in giudizio come testimone; d) quest'ultima deve avere una personale conoscenza dell'atto che ha trascritto; e) non devono esservi motivi tali da determinare la persona a registrare gli atti in maniera irregolare (83).

Occorre ora tener presente anzitutto che l'informazione computerizzata è contenuta in schede perforate o in bande magnetiche le quali, per essere leggibili, devono essere trascritte in stampati.

Le difficoltà a far rientrare i dati forniti dal computer nelle regole che prevedono eccezioni al principio generale della testimonianza umana sono di tre tipi: a) la registrazione può non costituire un'operazione di « routine »; b) può essere stata effettuata molti giorni dopo i fatti; c) può essere stata effettuata da un certo numero di persone molte delle quali non hanno conoscenza diretta e personale dei fatti.

Le Corti Statunitensi, comunque, sono molto riluttanti ad ammettere come fonti di prova le informazioni fornite dai computers ed, in genere, hanno assunto posizione molto rigoristiche al riguardo, il che ha favorito indirettamente i *computer-criminals* (84).

Alcuni Stati, tuttavia, come il North Carolina ed il Delaware, hanno adottato norme che prevedono specificamente i problemi relativi alle controversie nascenti dall'uso dei computers.

A livello federale è stato emanato poi nel 1977 il *Federal Computer System Protection Act* il quale potrebbe risolvere, almeno in parte, i problemi derivanti dai *computer-crimes* in quanto prevede tale atti come *felony*, punibili con pena detentiva fino ad un massimo di 15 anni o con pena pecuniaria fino a 50.000 dollari ovvero (punibili) con pena congiunta (85).

Gli Autori statunitensi, in particolare, esprimono forti preoccupazioni per l'impatto fra questa nuova forma di criminalità ed il sistema di *law enforcement* specie in termini di costi e

---

(83) BEQUAI, *op. cit.* alla nota 6.

(84) BEQUAI, *op. cit.* alla nota 9), p. 128.

(85) BEQUAI, *op. cit.* alla nota 9), p. XII, 44, 45.

di tempo. A parte le difficoltà relative alle investigazioni preliminari, i processi per crimini del genere, infatti, si sono dimostrati molto più costosi, lunghi e complicati dei processi per altri delitti. Di solito vi sono documentazioni voluminosissime, grande numero di testimoni ed interi eserciti di avvocati. Fino ad oggi sono stati pochi i giudici che sono riusciti a trovare i fondi e la forza necessaria per portare a termine processi di questo genere.

Secondo gli esperti, un caso complicato di *computer crime* potrebbe benissimo causare il collasso di un piccolo ufficio inquirente. Se non si provvederà a ridurre i costi dei processi per questo tipo di crimine i *computer-criminals* finiranno per rimanere impuniti per il solo motivo che sarebbe troppo costoso incollarli (86).

10. — Molta responsabilità nella commissione dei *computer-crimes* viene fatta risalire alle Case costruttrici di computers le quali, in genere, non hanno previsto sistemi di sicurezza per impedire o ridurre il pericolo di manipolazioni dei dati e di intercettazione degli stessi. È soltanto da poco che le predette Case, sotto la pressione dell'opinione pubblica, sollecitata a sua volta dal clamore suscitato da alcuni gravi casi di *computer crimes*, hanno cominciato a studiare ed, in qualche caso ad adottare, sistemi oggettivi di sicurezza (87).

Un'eguale parte di responsabilità grava, però, anche sui proprietari di « computers » i quali hanno trascurato di adottare alcune indispensabili precauzioni.

La situazione è stata posta molto bene in luce da esperti della *Data Security Holding*, una società americana specializzata nell'accertamento e nella prevenzione dei *computer-crimes* (88). Altri rilievi molto importanti in ordine alle deficienze dei sistemi di sicurezza sono emersi in un seminario tenutosi a

---

(86) BEQUAI, *op. cit.* alla nota 5, p. 172. I rilievi e le conclusioni esposte nel testo hanno un valore anche maggiore per il sistema italiano ove poste in relazione alla grave situazione della giustizia penale.

(87) La SIEMENS ha realizzato un sistema detto GOLEM il quale prevede un particolare « controllo di autorizzazione » che permette di verificare se un determinato utente è autorizzato a consultare un certo tipo di informazioni registrate nell'archivio elettronico ed — in particolare — se l'utente può eseguire una certa procedura (BORRUSO, *op. cit.* alla nota 2), Vol. I, p. 231, ss.). Recentemente (novembre 1978) la IBM ha pubblicato una serie di volumetti dal titolo « *Data Security Design Handbooks* » e dei ciclostilati aventi ad oggetto le misure da adottare da parte dell'utente per la sicurezza dello EDP.

(88) MODULO, *op. cit.* alla nota 15.

Phoenix, Arizona, il 23 aprile 1976, sotto gli auspici anche del *Department of Commerce*, ed in particolare dalla relazione di JERRY LOBEL, manager della *Honeywell Corporation* (89).

Gli specialisti del settore hanno comunque elaborato una serie di regole e di precauzioni che le organizzazioni proprietarie di computers dovrebbero adottare. Anzitutto occorrerebbe separare i poteri e le responsabilità per cui, ad esempio, i programmatori non dovrebbero essere anche operatori. Gli impiegati dovrebbero essere, poi, frequentemente cambiati in modo che non ci sia nessuno di essi che possa avere accesso al computer per un tempo molto lungo. Gli addetti al computer, inoltre, non dovrebbero avere accesso alla cassa ed agli inventari delle merci, né dovrebbero avere il potere di firmare chèques, ordini di acquisto o bolle di spedizioni. Tutte le istruzioni dovrebbero essere date per iscritto, comprese quelle fornite dai programmatori agli operatori. Le responsabilità di preparare, autorizzare, modificare e gestire i programmi dovrebbero essere separate il più possibile.

Ogni cambiamento di programma dovrebbe essere registrato e la data, il motivo ed il *cross reference* dovrebbero essere annotati. Tutti i documenti inviati alla *computer room* per l'*input - processing* dovrebbero essere attentamente controllati.

Le comunicazioni tra computer e terminali, così come tra computer e computer, dovrebbero essere in codice ed i *passwords* dovrebbero essere frequentemente cambiati, in modo da limitare il danno nel caso in cui un criminale venisse in possesso di un codice.

Speciali precauzioni dovrebbero anche essere prese nel caso di trasmissione di dati di natura segreta (es., macchine crittografiche). Il sistema dovrebbe, poi, poter registrare i tentativi infruttuosi di entrata nel sistema stesso, in modo da poter avvisare l'organizzazione che il suo computer è « sotto attacco ».

Infine il computer dovrebbe essere programmato per interrompere il contatto con i terminali dopo un determinato periodo di inattività degli utenti dei terminali stessi (90).

---

(89) U. S. DEPARTMENT OF COMMERCE, *Crimes Against Business*, Washington, nov. 1976, p. 22.

(90) BEQUAI, *op. cit.* alla nota 6) ed alla nota 9), p. 19-24. Vedi anche PARKER, *op. cit.* alla nota 3), p. 275-289; LEIBHOLZ-WILSON, *op. cit.* alla nota 48), p. 53-98.

11. — Gli esperti prevedono che l'attuazione dell'EFT farà senz'altro aumentare la commissione dei *computer-crimes* e ciò sia da parte di privati che da parte di organizzazioni criminali.

Aumenteranno anzitutto i furti di dati e delle informazioni. Infatti i computer dell'EFTS conterranno moltissimi dati importanti riguardanti singoli e società ed anche informazioni confidenziali o riservate riguardanti singoli, società ed istituzioni.

Tali informazioni potrebbero avere un grandissimo valore per i ricattatori, per i membri dell'anonima sequestri, per le ditte concorrenti, per gli avversari politici, per gli istituti di credito e perfino per gli estremisti politici.

In certi ambienti si sarebbe disposti a versare forti somme in cambio di informazioni, segreti industriali o dati su personalità politiche (91).

Si avrebbe quindi un ampio campo di attività per il crimine organizzato in conseguenza dell'ulteriore sviluppo del mercato nero delle informazioni e dei dati. Anche le falsificazioni e le manipolazioni dei dati e delle informazioni potrebbero conoscere un ampio sviluppo.

Attualmente esistono documentazioni cartacee relative alle operazioni le quali costituiscono una prova di tali operazioni. Con il sistema del EFTS i criminali, con l'aiuto di complici all'interno di una Banca, potrebbero, ad es., costituire dei falsi conti e stipulare le relative transazioni ed anche creare venditori e compratori fittizi. La possibilità di trasferimenti internazionali di somme nel giro di qualche minuto, renderebbe difficoltosa, se non addirittura impossibile, la scoperta di simili reati il che finirebbe per creare una diffusa sfiducia nel sistema stesso.

Anche altri delitti, come le appropriazioni indebite, aumenteranno giacché con l'aiuto del sistema, persone sia all'interno dell'organizzazione che all'estero della stessa, e con possibilità di accesso ad un terminale, potranno effettuare trasferimenti di fondi, forniture e materiali.

Il furto di tesserini di identificazione assumerà un notevole sviluppo insieme alla loro falsificazione ed al loro spaccio, il che attaccherà, per così dire al cuore, lo stesso sistema EFTS (92).

---

(91) BEQUAI, *op. cit.* alla nota 5), p. 166.

(92) BEQUAI, *op. cit.* alla nota 5), p. 66, ss.

Sarà praticamente impossibile sorvegliare la miriade di calcolatori, tenendo conto anche della diversità delle eventuali misure di sicurezza adottate da ciascun componente del sistema.

Anche la possibilità per l'emittente di assegni, di bloccare il pagamento degli stessi prima dell'incasso non esisterà più. Infatti, con l'EFTS i fondi saranno trasferiti dal conto dell'emittente a quello del delinquente nel giro di pochi minuti e senza che all'emittente dell'assegno rimanga prova di avere effettuato il pagamento ad una determinata persona, il che creerà immense complicazioni nel caso di pagamenti effettuati all'estero.

Infine con l'EFTS aumenteranno considerevolmente il numero e la qualità delle intercettazioni elettroniche e, probabilmente, data la posta in gioco, si svilupperà una tecnologia sofisticatissima al riguardo.

In definitiva con l'avvento dell'EFTS si creerà un modo di vivere nel quale l'uso della carta moneta diventerà quasi eccezionale. I conti potranno essere pagati semplicemente formando un numero telefonico e dando istruzioni al computer di una banca di trasferire i fondi dal proprio conto a quello del creditore (93).

Le rapine a mano armata potrebbero scomparire ma per essere sostituite da nuove forme di criminalità le quali, a loro volta, richiederebbero l'impiego di apparati di investigazioni e di perseguimento altamente specializzati ed efficienti. L'attuale sistema di *law enforcement*, già in gravi difficoltà nel perseguimento dei crimini ordinari, probabilmente si troverebbe del tutto impreparato a fronteggiare la criminalità derivante dalla « *cashless society* » e potrebbe rischiare il collasso (93 bis).

Gravissimi problemi inoltre si creerebbero per la « *privacy* » degli individui. La vita privata potrebbe divenire un libro aperto per i governi, per gli istituti di credito e per i criminali (94).

12. — Come già si è accennato, la società occidentale diventa sempre più dipendente dal sistema EDP e tale dipendenza

---

(93) BEQUAI, *op. cit.* alla nota 9), p. 181, ss.

(93 bis) Sui problemi legali connessi con i *computer crimes*, vedi NYCUM, *Computer Abuses raise new legal problems*, in Amer. Bar. Assoc. 1975, n. 61.

(94) BEQUAI, *op. cit.* alla nota 9, p. 192.

sarà fortemente accentuata dall'attuazione intensiva dell'EFTS in un futuro molto prossimo.

La gestione di un siffatto sistema ed il controllo del nuovo tipo di criminalità *white collar* in precedenza descritta diventeranno sempre più un problema sociale, oltre che criminologico e giudiziario. Sul piano economico, le perdite collegate ai *computer-crimes* sono in costante aumento e, come si è visto, in casi singoli possono raggiungere somme astronomiche mentre le « cifre nere » di tale forma di criminalità raggiungono percentuali altissime.

Lo sviluppo incontrollato del tipo di criminalità *by computer* già definito come: « *the crime of futur* », potrebbe avere gravi ripercussioni sociali. Anzitutto una diffusa sfiducia da parte del pubblico nel sistema EFTS, il cui sviluppo appare assolutamente indispensabile per governare sistemi, la gestione dei quali richiede in modo vitale una più completa automatizzazione dei dati e delle informazioni. Appare infatti impensabile una gestione del settore aziendale, di quello burocratico e di quello militare con i metodi tradizionali.

L'accertamento ed il perseguimento della forma di criminalità in oggetto diventerebbero, tenendo conto anche dell'immediatezza dei trasferimenti internazionali di somme e dell'ingresso sempre più massiccio nel settore del crimine organizzato, una impresa disperata per il sistema giudiziario penale del mondo occidentale.

I sistemi penali e giudiziari occidentali, infatti, sono stati progettati per la repressione della delinquenza tradizionale, quella cioè delle classi sociali inferiori. Ora i criminali *white collar* ed in particolare i *computer-criminals*, appartengono in genere ad una *élite*, nel caso di specie, tecnologica. Essi costituiscono, come concisamente ha affermato A. BEQUAI, « *the cream of our technological world* ».

Il lento ed antiquato sistema legale e giudiziario occidentale non è in grado attualmente di affrontare la « sfida tecnologica » della nuova criminalità. Occorre che la criminologia inizi al più presto a studiare in modo approfondito la criminalità correlata all'uso del computer, uscendo dai suoi schemi tradizionali. Tale tipo di criminalità è stata infatti oggetto di indagini soltanto a partire dalla fine degli anni '60, prevalentemente

ad opera di esperti di informatica e di diritto penale, americani e tedeschi (95).

Gli aspetti molteplici e complessi dei *computer-crimes* esigono, peraltro, ricerche interdisciplinari: i criminologi dovranno pertanto collaborare con gli esperti d'informatica, con gli economisti, i sociologi, gli psicologi ed i penalisti. Tali ricerche potrebbero sensibilizzare l'opinione pubblica, sino ad oggi tollerante nei confronti della criminalità *white collar*, e costituire la base per le riforme dei sistemi legali e giudiziari nazionali e per la instaurazione di una efficace collaborazione internazionale nel settore, indispensabili per affrontare con un minimo di successo la minaccia dei *computer-criminals* i quali, come ha affermato A. BEQUAI, sfidano « *not only our imagination, but also our system of Justice* ».

---

(95) L'argomento relativo alla criminalità degli affari è attualmente allo studio presso il Consiglio d'Europa ad opera di un apposito comitato ristretto del C.E.P.C. Non sembra però, che il Comitato abbia, almeno sino ad oggi, dedicato molta attenzione al fenomeno dei *computer-crimes*, pur essendosi in Europa verificatisi non pochi casi di simili illeciti.

Nell'ultima sessione plenaria del C.E.P.C., tenutasi a Strasburgo dal 19 al 23 marzo di quest'anno, chi scrive ha richiamato l'attenzione dei vari delegati sull'opportunità di dedicare appositi studi e indagini a questa nuova e pericolosissima forma di « criminalità tecnologica ».

## RIASSUNTO

L'avvento del computer ha determinato la creazione di un nuovo ambiente tecnologico nel mondo degli affari la cui dipendenza dall'EDP (Electronic Data Processing) appare ormai un fatto innegabile. Tale dipendenza sarà pressoché totale allorché sarà attuato su larga scala il sistema denominato EFTS (Electronic Funds Transfer System) il quale consentirà una pressoché completa automazione delle transazioni e dei processi commerciali.

Lo sviluppo di siffatta tecnologia è stato accompagnato, però, dal sorgere di una nuova forma di criminologia « *white-collar* » denominata « *computer-related-crime* » o più brevemente, « *computer-crime* », la quale ha per oggetto o per strumento appunto il computer. Il « *computer-crime* » però assume varie forme delle quali si tenta una classificazione basandosi sullo scopo dell'azione criminosa.

La classificazione è accompagnata da un'abbondante casistica, relativa soprattutto agli Stati Uniti ed alla Repubblica Federale di Germania, Paesi nei quali il crimine in oggetto ha assunto proporzioni più vistose ed allarmanti. Viene poi tracciato il profilo psicologico del « *computer-criminal* » con riferimento alle indagini compiute da Parker e da Bequai negli Stati Uniti e da Tiedemann e Sieber in Germania, indagini dalle quali emerge che il « *computer criminal* » è anch'esso un « raffinato prodotto » del progresso tecnologico nel settore degli affari.

È indubbia la pericolosità sociale di siffatta forma di criminalità, ove si tenga conto dell'elevatissimo « *dark number* » e del costo devastante dei « *computer-crimes* ».

L'attuazione dell'EFTS farà prevedibilmente aumentare il tipo di criminalità in oggetto, con correlativa diminuzione di quella tradizionale relativa ai delitti contro il patrimonio.

Il controllo della criminalità «by computer» diventerà sempre più un problema sociale, oltre che criminologico e legale. I sistemi giudiziari del mondo occidentale, progettati per la repressione della criminalità tradizionale, non sembrano in grado — però — di affrontare questo tipo di «sfida tecnologica».

La criminologia, e particolarmente quella sua speciale branca denominata «criminologia economica», dovrebbe affrettarsi a studiare il fenomeno in modo approfondito, anche mediante ricerche interdisciplinari; ciò in considerazione degli aspetti molteplici e complessi dei «computer-crimes».

I risultati di tali ricerche potrebbero sensibilizzare l'opinione pubblica, sinora tollerante nei confronti di siffatto tipo di criminalità, e costituire la base per le necessarie ed urgenti riforme delle legislazioni nazionali e per la instaurazione di una stretta collaborazione sul piano internazionale, necessarie per una efficace repressione del nuovo tipo di criminalità.

## RESUME

L'avènement de l'ordinateur a entraîné la création d'un nouveau milieu technologique dans le monde des affaires, dont la dépendance de l'EDP (Electronic Data Processing) apparaît désormais un fait incontestable. Cette dépendance sera presque totale lorsqu'on utilisera à grande échelle le système dénommé EFTS (Electronic Funds Transfer System), qui permettra une automation presque totale des transactions et des procédés commerciaux.

Le développement de cette technologie a entraîné toutefois une nouvelle forme de criminologie «white-collar» dénommée «computer-related-crime» ou, plus brièvement, «computer-crime», ayant pour objet ou pour instrument justement l'ordinateur. Mais le «computer crime» prend plusieurs formes, dont on essaie de faire un classement en se basant sur le but de l'action criminelle.

Ce classement s'accompagne de nombreux cas criminels, concernant principalement les Etats-Unis et la République Fédérale d'Allemagne, pays dans lesquels le crime dont il est question a pris des proportions plus considérables et alarmantes. L'Auteur trace ensuite le profil psychologique du «computer-criminal», en se référant aux enquêtes menées par Parker et Bequai aux Etats-Unis et par Tiedemann et Sieber en Allemagne: il sort de ces enquêtes que le «computer criminal» est, lui aussi, un «produit raffiné» du progrès technologique dans le domaine des affaires.

Cette forme de criminalité est sans doute très dangereuse pour la société, si l'on tient compte du «dark number» très élevé et du coût énorme des «computer-crimes».

La mise en oeuvre de l'EFTS fera très probablement augmenter le type de criminalité dont il est question, tandis qu'elle fera baisser la criminalité traditionnelle relative aux délits contre le patrimoine.

Le contrôle de la criminalité «by computer» deviendra de plus en plus un problème social, et non seulement criminologique et légal. Toutefois, les systèmes judiciaires du monde occidental, étudiés en vue de la répression de la criminalité traditionnelle, ne semblent pas à même de faire face à ce «défi technologique».

La criminologie, et surtout sa branche particulière dénommée «criminologie économique» devrait se hâter d'étudier ce phénomène d'une manière approfondie, même par des recherches interdisciplinaires; et cela à cause des aspects multiples et complexes du «computer-crime».

Les résultats de ces recherches pourraient sensibiliser l'opinion publique, jusque-là tolérante vis-à-vis de ce type de criminalité, et servir de base pour les réformes nécessaires et urgentes des législations nationales et pour la mise en oeuvre d'une étroite collaboration au niveau international, indispensables en vue d'une répression efficace du nouveau type de criminalité.

## SUMMARY

The advent of computers has brought about the creation of a new technological environment in the business world, whose dependence on EDP (Electronic Data Processing) seems now to be an undeniable fact. Such a dependence will be nearly total as soon as the system called EFTS (Electronic Funds Transfer System) will be realized on a large scale; this system will make it possible an almost complete automation of commercial transactions and processes.

The development of this technology was accompanied, however, by the growth of a new form of «white collar» criminology, called «computer-related time» or, more briefly, «computer-crime», whose object or tool is the computer itself. The «computer crime» assumes, however, a number of forms, of which a classification is attempted taking as a basis the purpose of the criminal action.

The classification is accompanied by a plentiful case-list, chiefly relating to the United States and to the Federal Republic of Germany, where the crime dealt with here has acquired more impressive and alarming proportions. The psychological outline is then sketched out of the «computer-criminal», with reference to the investigations carried out by Parker and by Bequai in the United States and by Tiedemann and Sieber in Germany, from which investigations there emerges that the «computer-criminal» is also a «sophisticated products» of the technological advance in the business sector.

The social dangerousness of such a form of criminality is undeniable, if one considers the exceedingly high «dark number», and the devastating cost of the «computer-crimes».

The implementation of EFTS will be likely to increase the type of criminality under discussion, with a related decrease of the conventional one concerning the crimes involving property.

The criminality control «by computer» will increasingly represent a problem not merely social but also criminological and legal. The judicial systems of the western world, planned for the repression of the conventional criminality, do not seem capable — however — to cope with this type of «technological challenge».

Criminology, and particularly that special branch of it called «economic criminology», should hasten to study in depth such a phenomenon, also through an interdisciplinary research work; this in view of the manifold and complex aspects of the «computer-crimes».

The results of these researches might alert the public opinion, so far tolerant towards such a type of criminality, and represents the basis for the necessary and urgent reforms of the national legislations and for the setting-up of a close cooperation at the international level, required for an effective repression of the new type of criminality.

## RESUMEN

El advenimiento del computer ha determinado la creación de un nuevo ambiente tecnológico en el mundo de los negocios cuya dependencia del EDP (Electronic Data Processing) aparece ya como un hecho innegable. Dicha dependencia sera casi total cuando se actuará en grande escala el sistema denominado EFTS (Electronic Funds Transfer System) el cual permitirá casi una completa automatización de las transacciones y de los procesos comerciales.

Por otro lado, el desarrollo de dicha tecnología ha sido acompañado por el nacimiento de una nueva forma de criminalidad «white-collar» denominada «computer-related-crime» o más brevemente, «computer-crime», la cual tiene por objeto o por instrumento justamente el computer. Sin embargo, el «computer-crime» asume varias formas de las cuales se trata de hacer una clasificación basandose sobre la finalidad de la acción criminal.

La clasificación está acompañada con una abundante casuística sobre todo relativa a los Estados Unidos y a la República Federal Alemana, países en los cuales el crimen en objeto ha asumido proporciones mas vistosas y alarmantes. Se traza luego el perfil psicológico del «computer-criminal» con referencia a las investigaciones realizadas por Parker y Bequai en los Estados Unidos y por Tiedemann y Sieber en Alemania, investigaciones de las cuales resulta que también el «computer-criminal» es «un producto refinado» del progreso tecnológico en el sector de los negocios.

Es indudable el peligro social de esta determinada forma de criminalidad si se tiene en cuenta el elevadísimo «dark number» y el costo devastador de los «computer-crimes».

Es de prever que la actuación del EFTS hara aumentar el tipo de criminalidad en objeto, con correlativa disminución de aquella tradicional relacionada con los delitos contra el patrimonio.

El control de la criminalidad «by computer» será siempre un problema social además que criminológico y legal. Mas los sistemas judiciales del mundo occidental, proyectados hacia la represión de la criminalidad tradicional, no parecen estar en grado de enfrentar este tipo de «desafío tecnológico».

La criminología y particularmente aquel ramo denominado «criminología económica», debería apurarse en el estudio profundizado del fenómeno, a un mediante investigaciones inter disciplinarias, lo cual es necesario considerando los múltiples y complejos aspectos del «computer-crimes».

Los resultados de dichas investigaciones podrían sensibilizar la opinión pública hasta el momento tolerante con dicho tipo de criminalidad y constituye la base para las necesarias y urgentes reformas de las legislaciones nacionales y para la instauración de una estrecha colaboración a escala internacional, necesarias para una eficaz represión del nuevo tipo de criminalidad.

## ZUSAMMENFASSUNG

Die Erfindung des Computers hat die Schaffung eines neuen technologischen Bereich in der Geschäftswelt geschaffen, deren Abhängigkeit vom EDP (Elektronik Data Processing) nummehr eine unleugbare Tatsache ist. Diese Abhängigkeit wird fast vollkommen total sein, da auf breiter Basis das System, genannt EFTS (Electronic Funds Transfer System) angewendet werden wird, das eine fast komplette Automatisierung der Transaktionen und der Handelsprozeduren erlauben wird.

Die Entwicklung einer solchen Technologie ist jedoch begleitet vom Aufkommen einer neuen Form von Kriminalologie «white-collar», genannt «computer-related-crime» oder in kürzerer Form «computer-crime», die als Objekt oder Instrument eben gerade den Computer hat. Der «computer-crime» nimmt jedoch verschiedene Formen an, von denen man versucht, sie zu klassifizieren, indem man sich auf den Zweck der kriminellen Handlung basiert.

Die Klassifizierung wird begleitet von einer zahlreichen Kasistik, bezüglich besonders auf die Vereinigten Staaten und auf die Deutsche Bundesrepublik, Länder in denen das genannte Verbrechen ansehnliche und alarmierende Ausmasse angenommen hat. Es wird sodann das psychologische Profil des «computer-criminal» aufgezeigt in bezug auf die Untersuchungen, welche von Parker und Bequai in den USA und von Tiedemann und Sieber in Deutschland durchgeführt wurden, Untersuchungen, aus denen hervorgeht, dass das «computer-criminal» ebenfalls ein «raffiniertes Produkt» des technologischen Fortschritts auf dem Sektor der Geschäfte ist.

Die Gefährlichkeit in sozialer Hinsicht einer solchen Form von Kriminalität ist ohne Zweifel dort, wo man Rechnung trägt der sehr hohen «dark number» und der verwüstende Preis der «computer-crimes».

Die Anwendung des EFTS wird voraussichtlich die betreffende Kriminalität steigern während sie eine Verminderung jener traditionellen zur Folge haben wird, die sich auf die Verbrechen gegen das Vermögen beziehen.

Die Kontrolle der Kriminalität «by computer» wird immer mehr ein soziales Problem werden, sowie ein kriminelles und gesetzliches. Die Justizsysteme der westlichen Welt, projektiert für die Unterdrückung der traditionellen Kriminalität, scheinen jedoch nicht fähig zu sein, diesem Typ der «technologischen Herausforderung» zühn entgegenzutreten.

Die Kriminalogie und besonders ihr spezieller Bereich, genannt «wirtschaftliche Kriminalogie», müsste sich beeilen, das Phänomen auf profundierte Art und Weise zu studieren, auch durch interdisziplinäre Forschungen; das heisst die vielfachen Aspekte und Komplexe der «computer-crimes» in Betracht zu ziehen.

Die Ergebnisse dieser Forschungen könnten die öffentliche Meinung sensibilisieren, die bisher im Vergleich zu diesem Typ von Kriminalität tolerant war und bildet auch die Basis fuer die nötigen und dringenden Reformen der nationalen Gesetzgebung und für die Instauration einer engen Zusammenarbeit auf internationaler Ebene, welche nötig ist für eine wirksame Repression dieses neuen Typs von Kriminalität.